UNIVERSIDAD POLITECNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERIA DE SISTEMAS

Proyecto Técnico previo a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

REORGANIZACIÓN DEL DIRECCIONAMIENTO LÓGICO E IDENTIFICACIÓN DE VULNERABILIDADES EN LA RED INTERNA PARA LA IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PERIMETRAL EN LA GOBERNACIÓN DEL GUAYAS

AUTORES:

ANA BEATRIZ BARRAGÁN ROJAS

KAVIR JUDSON CUADROS LOOR

TUTOR:

ING. DANNY BARONA, MBA.

Guayaquil, septiembre de 2019

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotros, **ANA BEATRIZ BARRAGÁN ROJAS** y **KAVIR JUDSON CUADROS LOOR**, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaramos que los conceptos y análisis desarrollados, y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

---	---
ANA BEATRIZ BARRAGÁN ROJAS	KAVIR JUDSON CUADROS LOOR
C.I: 0951962224	C.I.: 0924836711

CESIÓN DE DERECHOS DE AUTOR

Nosotros, **ANA BEATRIZ BARRAGÁN ROJAS** y **KAVIR JUDSON CUADROS LOOR** con documento de identificación Nº **0951962224** y **0924836711** respectivamente, manifestamos nuestra voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del proyecto técnico titulado *"Reorganización del direccionamiento lógico e identificación de vulnerabilidades en la red interna para la implementación de mecanismos de seguridad perimetral en la Gobernación del Guayas"*, el mismo que ha sido desarrollado con la finalidad de obtener el título de: Ingeniero en sistemas, en la Universidad Politécnica Salesiana. La Universidad queda facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Prioridad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscrito este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

---	---
ANA BEATRIZ BARRAGÁN ROJAS	KAVIR JUDSON CUADROS LOOR
C.I: 0951962224	C.I.: 0924836711

CERTIFICADO

Yo declaro que bajo mi tutoría fue desarrollado el trabajo de titulación "REORGANIZACIÓN DEL DIRECCIONAMIENTO LÓGICO E IDENTIFICACIÓN DE VULNERABILIDADES EN LA RED INTERNA PARA LA IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PERIMETRAL EN LA GOBERNACIÓN DEL GUAYAS", realizado por **Ana Beatriz Barragán Rojas** y **Kavir Judson Cuadros Loor**, obteniendo el Proyecto Técnico, que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana.

Ing. Danny Barona
Universidad Politécnica Salesiana,
Sede Guayaquil

DEDICATORIA

A mi familia, en especial a las tres personas más importantes de mi vida, mi mamá, Martha Alexandra Rojas Caranqui, quien desde pequeña me enseñó el significado del sacrificio y la perseverancia, y a quien deseo recompensar por todo su apoyo y amor incondicional.

A mi esposo, Gandhi Marcelo Navarrete Abad, quien siempre estuvo pendiente y me dio su mano durante el transcurso de la elaboración de este proyecto, quien me permitió traer al mundo a la tercera persona a quien dedico mi esfuerzo diario, al amor de mi vida, mi hija Annie Guadalupe Navarrete Barragán: nunca dudes de lo que sería capaz de hacer por y para ti.

A los ángeles que Dios puso en mi camino y que de una u otra forma colaboraron en cada detalle para culminar con el presente.

Ana Barragán Rojas

DEDICATORIA

A mi madre Mirian, quien a pesar de las adversidades que se han presentado a lo largo de su vida ha sabido ser un apoyo incalculable, una consejera precisa, una amiga constante y quien me ha llevado a ser lo que soy hoy en día.

A mi hija Luciana, quien con su afecto y cariño ha sido el detonante de mi felicidad, de mi esfuerzo y mis ganas de buscar lo mejor para ella. Aún a su corta edad me ha enseñado muchas cosas y lo seguirá haciendo.

A German, quien cumplió el rol de padre y supo darme los lineamientos para ser una persona íntegra y responsable.

Kavir Cuadros Loor

AGRADECIMIENTO

A todos quienes de forma directa o indirecta contribuyeron a la realización de este trabajo, no podría nombrar a todos de forma particular, pero si quiero recalcar que cada uno de ellos con cada palabra de aliento y de sabiduría estuvieron fortaleciendo mis sentidos para poder llevar a cabo este proyecto.

También agradezco la colaboración del departamento de TIC's de la Gobernación del Guayas y todo el personal que me permitió culminar mi proyecto en la institución a pesar de ya no formar parte de ella.

Agradezco infinitamente a Dios por haberme permitido llegar al final de esta meta, puesto que él con sus bendiciones diarias han guiado cada paso de mi vida.

Ana Barragán Rojas

AGRADECIMIENTO

Ante todo, doy gracias a Dios, que me dio la fortaleza necesaria para realizar este proyecto y culminar mi carrera universitaria a pesar de las adversidades.

Gracias, al Ing. Danny Barona, por su total colaboración a lo largo del desarrollo de este trabajo y por estar dispuesto a brindarnos su orientación en todo momento.

Gracias a mi madre, quien me apoyo siempre, me impulsó en cada paso que he dado, por formarme, por confiar en mí, por inculcar todos los valores y pasiones que tengo. Gracias a ella estoy aquí, soy su fiel reflejo

Gracias a mi hija, quien me ayudo a encontrar el lado dulce y no amargo de la vida. Fue mi motivación más grande para concluir con éxito este proyecto.

Gracias, a la Gobernación del Guayas por permitirnos desarrollar en sus instalaciones, en especial al Ing. Henry De la Cruz y al Sr. Christian Ayala. Agradecido por su colaboración, paciencia y confianza.

Gracias, a la Universidad Politécnica Salesiana, por formarme como profesional, crecer como persona, como buen cristiano y ciudadano honrado. Gracias a los maestros que tuve, sus enseñanzas me permitieron alcanzar esta meta.

Gracias a mi compañera Ana Barragán, con quien pasamos adversidades durante el desarrollo de nuestro trabajo de titulación, las cuales pudimos sobrellevar y salir adelante con mucho esfuerzo.

Gracias a todos que de alguna manera intervinieron en el desarrollo del presente proyecto, a cada uno de ustedes mi más sincero agradecimiento.

Kavir Cuadros Loor

RESUMEN

La infraestructura de TI de una organización permite la administración del recurso humano (personal del área de Tecnología), así como de las plataformas tecnológicas: hardware, software, redes y bases de datos, con el fin de brindar un servicio de calidad a los usuarios cumpliendo con los objetivos estratégicos de la institución, misión y visión, optimizando todos sus recursos.

Cuando se implementa una infraestructura tecnológica de alta disponibilidad de servicio, los servicios informáticos que brinda la institución deben ser capaces de solventar la concurrencia de los usuarios, y es allí donde se busca preservar y cuidar de la seguridad del activo más importante dentro de toda institución, sea esta pública o privada, la información, basándose en los tres pilares fundamentales que implica la seguridad de ésta que son: la integridad, confidencialidad y disponibilidad.

El proyecto surge de la necesidad que tiene la institución de contar con un nivel de protección robusto a nivel físico y lógico, permitiendo de esta forma la implementación de un Gestor Unificado de amenazas con el fin de mitigar y solucionar las debilidades del sistema, las que se encontrarán en el levantamiento de la información y estudio previo, mediante el uso de una herramienta de escaneo y análisis de vulnerabilidades.

Con el fin de complementar una infraestructura uniforme, se realizó la reestructuración del direccionamiento de la red, así como la aplicación de estándares de cableado estructurado ANSI/TIA/EIA, que indican los requisitos mínimos que debe disponer una red interna dentro de una institución, para facilitar de esta forma la administración, detección y resolución de problemas de comunicaciones.

En el presente documento se podrá observar todas las etapas que se cumplieron para culminar con la implementación del proyecto y los resultados y recomendaciones para con la empresa.

ABSTRACT

IT infrastructure of an organization allows management of human resources (staff Technology area) as well as technology platforms: hardware, software, networks and databases, in order to provide quality service to users complying with the strategic objectives of the institution, mission and vision, optimizing their resources.

When a technological infrastructure of high availability of service is implemented, the IT services provided by the institution must be able to resolve the concurrence of the users, and that is where it seeks to preserve and take care of the security of the most important asset in any institution , whether it public or private, the information, based on the three fundamental pillars that implies its security, which are: integrity, confidentiality and availability.

The project arises from the need of the institution to have a robust physical and logical protection, thus allowing the implementation of a Unified Threat Manager in order to mitigate and solve the weaknesses of the system, which will be found in the gathering of information and previous study, through the use of a tool for scanning and analyzing vulnerabilities.

In order to complement a uniform infrastructure, the restructuring of the network addressing was carried out, as well as the application of structured cabling standards ANSI / TIA / EIA, which indicate the minimum requirements that an internal network must have within an institution, to thereby facilitate the administration, detection and resolution of communication problems.

This document may observe all stages that were fulfilled culminating in project implementation and the results and recommendations to the company.

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ECUACIONES

1. Introducción

El presente proyecto se realizó con el fin de brindar soluciones de mejora a los servicios de toda la red de datos de la Gobernación de la Provincia del Guayas, así como la protección del recurso esencial dentro de la misma, la información.

Por otra parte, en el ámbito académico y profesional, como futuros Ingenieros en Sistemas, el interés versó en poner en práctica los conocimientos y experiencias en materia de seguridad de la información en pro de esta institución pública.

La fase inicial de fundamentos teóricos da respuesta a la contextualización de la investigación y proyecto a implementar.

En el marco metodológico, el levantamiento de la información se recopiló mediante una entrevista al servidor público responsable del área de Tecnología y una serie de encuestas realizadas al personal de la institución, con el propósito de identificar problemas y oportunidades de mejora, así como definir los objetivos claves dentro del proyecto:

- Reestructurar el direccionamiento IP para establecer un nivel de protección robusto basado en buenas prácticas que abarque tanto a usuarios internos, externos y servidores.
- Identificar las vulnerabilidades de la red interna para mitigar el impacto de los ataques.
- Aplicar normas ANSI/TIA/EIA para la administración de cableados y puertos asignados a usuarios en dispositivos capa 2, para garantizar la conectividad de red entre usuarios de la red.

En la etapa de Análisis, se revisan, comparan y eligen los instrumentos de obtención de la información que se evaluarán con el fin de comprender la situación actual en su totalidad.

En el Diseño, se esquematiza y representa la solución de cada punto dentro del proyecto; durante la Implementación se ejecutó el trabajo experimental y desarrollo de tareas y actividades, así como la muestra de los resultados obtenidos en cumplimiento de los objetivos planteados con la institución.

2. Problema

La Gobernación del Guayas, cuenta con un diseño lógico de la red interna básica, deficiente y no ha sido debidamente planificada.

Dentro de la gobernación se han presentado varios problemas con ciertos usuarios que pueden acceder a los archivos de departamentos a los que no pertenecen, revisar la información y hasta manipular documentos importantes; el Despacho del Gobernador es el área más comprometida debido a la información que maneja.

En la red de datos de la Gobernación, la solución a problemas tiende a tardar más de lo que debería, por ejemplo, cuando se quiere buscar un punto de red dañado; esto se debe a la falta de etiquetado y organización con su respectivo registro; provocando mucha insatisfacción a los usuarios.

La ausencia de un correcto esquema de direccionamiento IP, ha originado que los servicios y recursos de red se encuentren vulnerables al estar en el mismo rango y que cualquier persona con acceso a la red pueda utilizar recursos que deberían estar restringidos.

En última instancia está el entretenimiento en redes sociales y sitios indiferentes a lo profesional por parte de los usuarios en horas laborables, provocando un bajo desempeño no adecuado en sus actividades inherentes al trabajo.

2.1. Antecedentes

La Gobernación del Guayas es una institución gubernamental, cuenta con su planta central en Guayaquil, Intendencia en Samborondón y Jefaturas, Comisarías, y Tenencias Políticas de los cantones y parroquias alrededor de la provincia del Guayas. La problemática se limitará a la planta central, la misma que cuenta con aproximadamente 100 usuarios.

La planta central de la Gobernación del Guayas, ubicada en la Av. Malecón y Aguirre cuenta con 3 plantas: Planta baja, primer piso y segundo piso, los mismo que están divididos de la siguiente manera:

- **Planta baja:** 7 departamentos (Ministerio del Interior, Contraloría, Secretaría General, Bodega de Administrativo, Dirección Administrativa Financiera, Unidad Administrativa y Recepción)

- **Primer piso:** 5 departamentos (Unidad de Comunicación Social, Unidad de Talento Humano, Unidad de Asesoría Jurídica, Jefatura Política del Cantón Guayaquil y Frente Social); así como 2 salones para eventos: Salón Libertadores y Salón Simón Bolívar y 2 salas de reuniones.
- **Segundo piso:** 7 departamentos (Despacho del gobernador, Dirección de Seguridad Ciudadana, Dirección de Planificación e Inversión, Unidad de Tecnología de la Información y Comunicaciones, Bodega de TIC, Intendencia y Sub Intendencia General de la Provincia), 1 sala de videoconferencia: Sala de sesiones y el Data Center.

La red de datos del edificio no está basada en un esquema de red segura por lo que tiene problemas de congestión de tráfico debido a que el direccionamiento IP no ha sido debidamente planificado.

Los usuarios dentro de la Gobernación tienen acceso a internet y a la red interna; con respecto al internet los usuarios pueden navegar de manera libre y sin control alguno. Por otra parte, la red interna no cuenta con ningún tipo de seguridad razón por la cual se han notado varios inconvenientes en la red de datos, básicamente relacionados con virus, softwares maliciosos instalados en algunas estaciones de trabajo de manera no intencional, caídas del servidor, entre otras. Todo esto se ha ido dando por la ausencia de seguridad perimetral en la red de datos que resguarde la información de la institución.

2.2. Importancia y alcance

Los beneficiarios del proyecto serían los usuarios de la Gobernación del Guayas, quienes podrán tener acceso a los diversos servicios informáticos de manera segura a través de todas las reglas de seguridad que se definirán en conjunto con el área pertinente, Unidad de Tecnología de la Información y Comunicación bajo aprobación de la Autoridad Máxima de la Institución, Gobernador de la Provincia del Guayas.

El Departamento de Tecnología también será beneficiado ya que gracias a la implementación de este proyecto podrán tener un mejor control sobre el tráfico de red, los niveles de manejo de información, las limitaciones de navegación y ancho de

banda; de igual manera con la aplicación de la Norma ANSI/TIA/EIA 606A la cual ayudará a tener una mejor administración del cableado estructurado.

2.3. Delimitación

El Gestor Unificado de Amenazas será implementado en la Gobernación del Guayas, edificio de Planta Central, ubicado en las calles Avenida Malecón y Calle Aguirre.

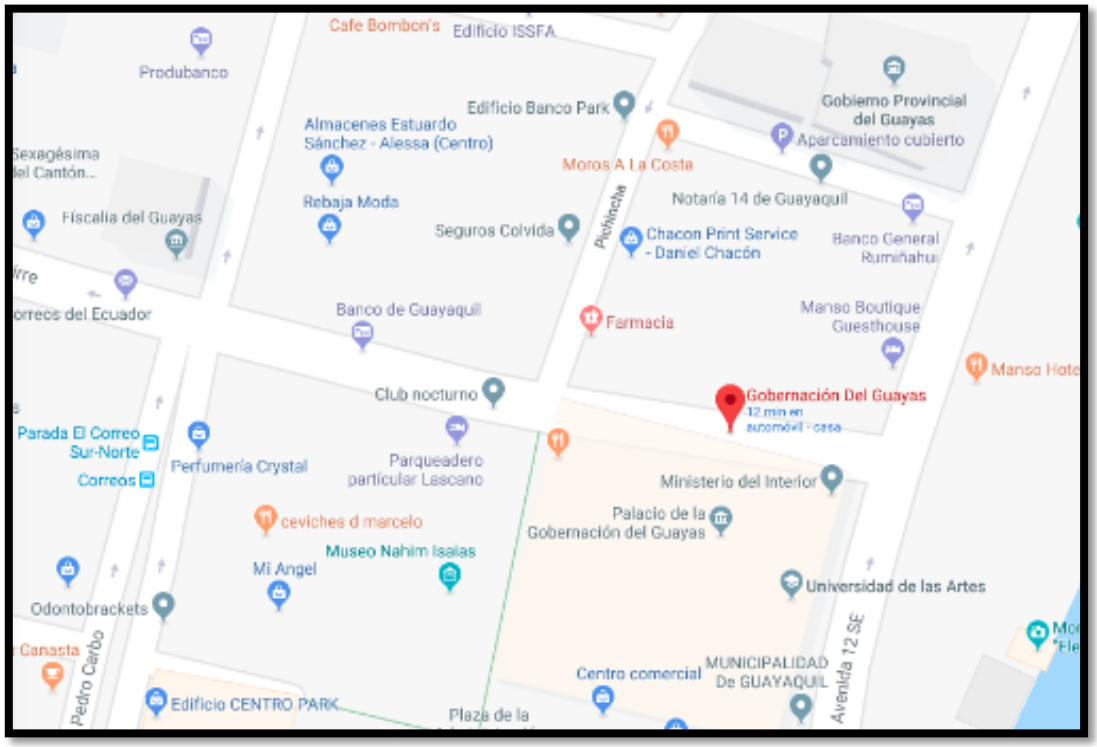


Figura 1. Ubicación del edificio de la Gobernación del Guayas
Obtenido de: (Google, 2019)

2.4. Presupuesto

Durante el desarrollo del presente proyecto, se determinó que, para la implementación y obtención de los resultados esperados basados en los objetivos específicos, será necesario la adquisición de lo siguiente:

Tabla 1. Presupuesto

No.	Descripción	Cantidad	Precio Unitario	Total
1	Sophos SG 210 Appliances + Suscripción anual	1	$ 5.479,04	$ 5.479,04
2	Etiquetadora de cable de red EPSON	1	$ 120,00	$ 120,00
3	Cintas para etiquetadora	8	$ 18,00	$ 144,00
4	Seguidor de tono, Tester LAN	1	$ 45,00	$ 45,00
5	Licencia Windows Server	1	$ 0,00	$ 0,00
6	Recurso humano	2	$ 100,00	$ 200,00
7	Materiales varios	-	$ 250,00	$250,00
TOTAL				**$ 6.238,04**

Elaborado por: Los autores

3. Objetivos

3.1. Objetivo general

Optimizar los servicios de la red de datos cableada e inalámbrica e implementar un Gestor Unificado de Amenazas en la Gobernación del Guayas.

3.2. Objetivos Específicos

- Reestructurar el direccionamiento IP para establecer un nivel de protección robusto basado en buenas prácticas que abarque tanto a usuarios internos, externos y servidores.
- Identificar las vulnerabilidades de la red interna para mitigar el impacto de los ataques.
- Aplicar normas ANSI/TIA/EIA para la administración de cableados y puertos asignados a usuarios en dispositivos capa 2, para garantizar la conectividad de red entre usuarios de la red.

4. Fundamentos teóricos

4.1. Modelos de comunicaciones

Los modelos de comunicaciones definen la implementación, estructuración y desarrollo, dividiendo en capas las tareas vinculadas a una transmisión, a fin de estandarizar las funciones a realizar en el intercambio de información entre sistemas computacionales; esta división permite delegar funciones específicas a cada una de las capas, obteniendo como resultado que los sistemas manejen estructuras por módulos. Los modelos de comunicaciones se clasifican en: Modelo OSI y Modelo TCP/IP.

4.1.1. Modelo Referencia OSI

Según (Tanebaum | Wetherall, 2012) este modelo se basa en una propuesta desarrollada por la Organización Internacional de Normas (ISO) como el primer paso hacia la estandarización internacional de protocolos utilizados en las diversas capas.

El modelo OSI se muestra en la Fig. 2, este modelo sirve para interpretar la funcionalidad de una red y como fluye el tráfico en la misma, así mismo sirve como guía en el desarrollo estándares, esquemas y dispositivos de red.

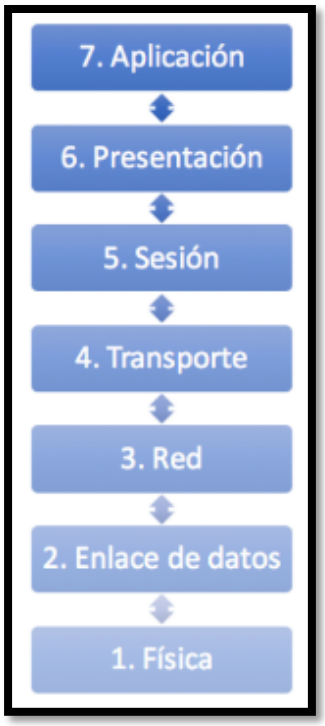


Figura 2. Modelo de Referencia OSI
Elaborado por: Los autores.

La descripción de las 7 capas según (Gerónimo, 2009) es la siguiente:

4.1.1.1. Capa física

Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto mecánico de la interfaz física.
- Describir el aspecto eléctrico de la interfaz física.
- Describir el aspecto funcional de la interfaz física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

4.1.1.2. Capa de Enlace de Datos

Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información para:

- Detectar error es en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para las sincronías.
- En general controla el nivel y las interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

4.1.1.3. Capa de Red

- Este nivel define el enrutamiento y el envío de paquetes entre redes.

- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una subred.
- Define el estado de los mensajes que se envían a nodos de la red.

4.1.1.4. Capa de Transporte

Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento.

- Garantiza una entrega confiable de la información
- Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por nivel 5 (Sesión).
- Este nivel define como direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío de mensaje.
- Establece la transparencia de datos, así como la confiabilidad en la transferencia de información entre dos sistemas.

4.1.1.5. Capa de Sesión

- Este nivel se encarga de proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.
- Establece el inicio y termino de la sesión.
- Recuperación de la sesión

- Control de diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

4.1.1.6. Capa de Presentación

- Traduce el formato y asigna una sintaxis a los datos para su transmisión en la red.
- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

4.1.1.7. Capa de Aplicación

- Proporciona servicio al usuario del Modelo OSI
- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencia de archivos (ftp), etc.

4.1.2. Modelo TCP/IP

Según (López, 2005) El modelo TCP/IP trata de un modelo más práctico destinado a su funcionalidad útil y directa, no como el modelo OSI más dirigido a presentar un marco teórico y completo de la interconexión de redes. La red Internet se apoya sobre la arquitectura del modelo TCP/IP de ahí su extrema importancia en la actualidad.

Este modelo maneja la misma lógica que el modelo OSI dividiendo sus niveles en capas, no obstante, define sus niveles de forma diferente como observaremos a continuación.

Tabla 2. Comparación de Modelo OSI y TCP/IP.

Modelo OSI	Modelo TCP/IP
Capa de aplicación	Capa de aplicación
Capa de presentación	
Capa de sesión	
Capa de transporte	Capa de transporte
Capa de red	Capa de Internet
Capa de enlace	Capa de acceso a la red (NAL)
Capa física	

Elaborado por: Los autores

4.1.2.1. Capa de acceso a la red

La capa de acceso a la red es la de nivel inferior, (Tanebaum | Wetherall, 2012) dice que enlaces como las líneas seriales y Ethernet clásica se deben llevar a cabo para cumplir con las necesidades de esta capa de interred sin conexión.

Esta capa se encuentra conformada por la capa de enlace de datos y la capa física, dentro de la misma están todos los componentes que necesita un paquete IP para completar un enlace físico.

4.1.2.2. Capa de internet

La capa de internet es la que permite a los hosts enviar paquetes a cualquier red y que se transporten de manera independiente al destinatario, se encarga de enrutar los paquetes evitando de esta manera congestiones de tráfico.

Esta capa define un formato de paquete y un protocolo oficial llamado IP, adicionalmente maneja un protocolo complementario llamada ICMP que le ayuda a funcionar.

4.1.2.3. Capa de transporte

La capa de transporte está diseñada para permitir una comunicación de extremo a extremo, es decir desde el nodo origen hacía el nodo de destino, en esta capa se definieron dos protocolos TCP y UDP.

El protocolo TCP, es un protocolo confiable y está diseñado para que el flujo de datos que envía una máquina sea recibido sin errores en cualquier máquina de la red interna.

El protocolo UDP, es totalmente contrario al TCP es un protocolo sin conexión y no confiable, cuando una máquina envía datos los mismo no son corroborados para saber si llegaron sin errores.

4.1.2.4. Capa de aplicación

En la creación del modelo TCP/IP se consideraron innecesarias las capas de sesión y presentación. Las aplicaciones ya deben incluir sus propias funciones de sesión y presentación si lo requieren.

La capa de aplicación maneja varios protocolos de alto nivel, como son TELNET que es el de terminal virtual, FTP para transferencia de archivos o SMTP para correo electrónico, a través de los años se han agregado muchos protocolos según (Tanebaum | Wetherall, 2012) La Figura 3, ilustra el modelo TCP/IP y sus protocolos más importantes en cada una de sus capas.

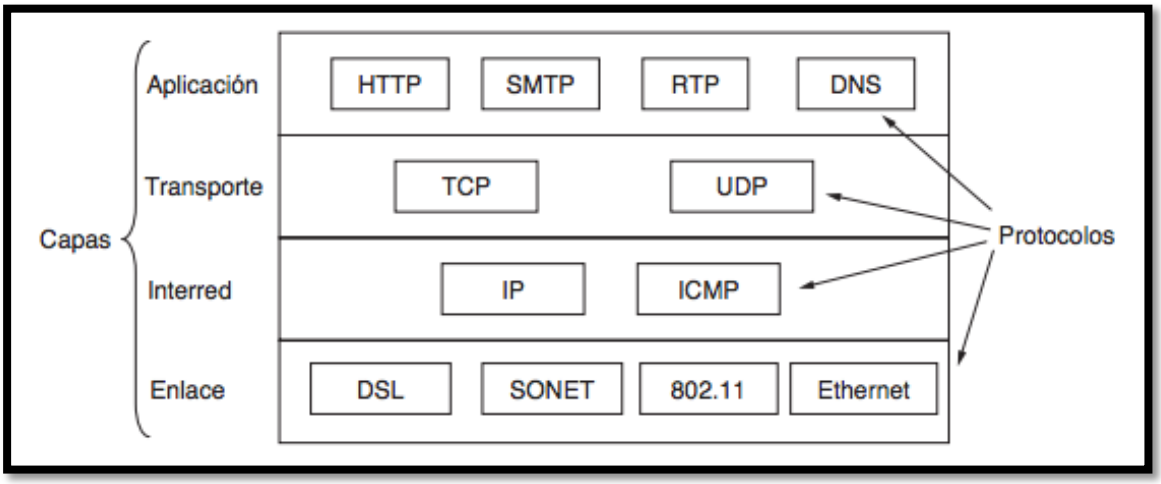


Figura 3. Modelo TCP/IP con algunos protocolos
Obtenido de: (Tanebaum | Wetherall, 2012)

4.2. Direccionamiento IP

(Andreu, 2014) define a una dirección IP como un número que identifica, de manera lógica y jerárquica, a una interfaz en red de un dispositivo que utilice el protocolo IP, que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión

utilizado, ni de la red. En la tabla, se muestra la clase de direcciones IP existentes de los rangos de cada una, y las aplicaciones:

Tabla 3. Clases de direcciones IP

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16777214	Redes grandes
B	128.0.0.0	191.255.255.255	16384	65534	Redes medianas
C	192.0.0.0	223.255.255.255	2097152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	NO APLICA	NO APLICA	Multicast
E	240.0.0.0	255.255.255.255	NO APLICA	NO APLICA	Investigación
*El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza					

Elaborado por: Los autores

4.2.1. Subnetting

El Subneteo consiste en dividir las direcciones full class en subredes, mediante las cuales se podrá tener una mejor organización de las redes grandes, así mismo se logrará contar con subredes adicionales y no será necesario ocupar más direcciones IP, con esto se reduce los dominios de broadcast en la red. Cuando se subnetea una red se elimina las conocidas “Clases de direcciones de red” y se habla de direcciones classless, las mismas que descomplican la administración y diseño de redes.

Subnetting consiste en coger prestados bits del host para crear las subredes nuevas, para esto se utiliza la siguiente fórmula:

- Cantidad de host por subred = 2^n-2
- Cantidad de subredes = 2^n-2
    - Donde n es el número de bits utilizados

Se restarán 2 porque cada subred tendrá una dirección de red y una dirección de broadcast.

Aunque el subnetting puede ser conveniente para algunos casos, no suele ser del todo eficiente debido a que todas las subredes se crean a partir de la original, por lo que tendrán la misma máscara de red, para optimizar esto se utiliza VLSM.

4.2.2. Máscara de Subred de Longitud Variable (VLSM)

VLSM permite utilizar más de una máscara de subred dentro de la misma red, además de optimizar la asignación de IP's, también ayuda a mejorar la capacidad de sumarización de rutas.

Para poder calcular las nuevas subredes se utiliza la misma fórmula que para subnetting, en donde los bits asignados para la parte de red definen también la máscara de red, a partir de la cual se determina la parte de host asignada.

Utilizando subnetting en las redes con un direccionamiento eficiente ya no tenemos el concepto de clase, ya que las máscaras varían.

4.3. VLAN

Una VLAN (Virtual Local Area Network) o Red de Área Local Virtual es un grupo flexible de dispositivos que se encuentran dentro de una red de área local en cualquier ubicación, pero se comunican como si estuvieran en el mismo segmento físico (Edwards, 2005).

Con las VLAN se puede segmentar la red sin limitarse a las ubicaciones o conexiones físicas.

Las principales ventajas que aportan las VLAN son:

- Mejor gestión de recursos y mayor flexibilidad, puesto que facilitan el cambio y movimiento de los dispositivos dentro de la red.
- Facilidad de localización y aislamiento de averías.
- Mayor seguridad, debido a la separación de dispositivos en distintas VLAN.
- Control de tráfico de broadcast.

Se pueden implementar atendiendo a diversos criterios como puertos de un switch a los que se conectan los ordenadores, direcciones MAC, etc.

4.3.1. Tipos de puerto en los switches

Existen dos tipos de puertos:

- Puertos de acceso: Se conectan las estaciones directamente. Mapean el puerto a una VLAN programada.
- Puertos 1Q Trunk: Se utilizan para conectar Switches entre sí y que pase el tráfico de diferentes VLAN a través de ellos.

4.3.2. VLAN nativas

Los fabricantes generalmente distribuyen sus equipos con la VLAN id 1 configurada como VLAN nativa, VLAN por defecto y VLAN de administración.

Esto quiere decir que, por defecto, todos los puertos del Switch pertenecen a la VLAN 1. Si un puerto es añadido a otra VLAN creada posteriormente, dejará por tanto de pertenecer a la VLAN de administración.

Solo se puede tener una VLAN nativa por puerto.

Las tramas pertenecientes a las VLAN nativas no se modifican cuando se envían por medio del trunking.

4.4. Seguridad Informática

Según (Aguilera, 2010) la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- Cuáles son los elementos que componen el sistema, información obtenida mediante entrevistas con los responsables o directivos de la organización y mediante apreciación directa.
- Cuáles son los peligros que afectan al sistema, sean estos accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y monitoreos.
- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales.

4.4.1. Tipos de seguridad

Seguridad Activa, es el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Seguridad Pasiva, está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema.

4.4.2. Análisis de riesgos

Según (Aguilera, 2010) a la hora de implementar seguridad a un sistema de información, se tomará en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema, para comenzar con el análisis hay que tener en cuenta los siguientes elementos:

4.4.2.1. Activos

Son los recursos que forman parte del sistema de información o que están relacionados con el mismo. Los activos se podrían calificar en los siguientes tipos:

- **Datos**. Son el núcleo de toda organización, se tiende a considerar que el resto de los activos están a servicios de los datos. Suelen estar organizados en bases de datos y almacenados en soportes de diferente tipo.
- **Software.** Conformado por los sistemas operativos y las aplicaciones instaladas en los equipos.
- **Hardware.** Conformado por los equipos que contienen las aplicaciones y permiten su funcionamiento, y almacenan los datos.
- **Redes.** Conformada por las redes locales de las organizaciones hasta la metropolitana o internet.
- **Soportes.** Donde los datos quedarán almacenados de manera permanente, puede ser desde un CD hasta disco duros externos.
- **Instalaciones.** Los lugares donde se encuentran ubicados los sistemas de información.
- **Personal.** El conjunto de personas que interactúan con el sistema de información.

- **Servicios.** Lo que se ofrece a clientes o usuarios, sean estos productos, sitios web, foros, correo electrónico, etc.

4.4.2.2. Amenazas

Según (Gascó, Serrano, & Ramada, 2013) una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. En función de las acciones realizadas por parte del atacante, las amenazas se clasifican en:

- **Amenazas pasivas,** tienen como objetivo obtener información relativa a una comunicación.
- **Amenazas activas,** tienen como objetivo realizar cambios no autorizados sobre el estado del sistema.

Otra posible clasificación sería en función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

- **De interrupción**. Tienen como objetivo deshabilitar el acceso a la información.
- **De intercepción.** Accesos no autorizados a recursos del sistema para captar información confidencial.
- **De modificación.** Acceso no autorizado y modificaciones a los programas y datos del sistema de información.
- **De fabricación**. Introducción de información falsa en el conjunto de información del sistema.

4.4.2.3. Riesgos

"Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad, ni vulnerabilidad cuando no existe amenaza para la misma." (Aguilera, 2010).

4.4.2.4. Vulnerabilidades

Se considera vulnerabilidad a las debilidades que tenga un activo que pueda afectar de cualquier manera al funcionamiento del sistema de información. Las

debilidades puedes estar relacionadas con fallos al momento de la implementación de aplicaciones o en la configuración de un sistema operativo, descuidos en usos de los sistemas, etc.

4.4.2.5. Ataques

Cuando un sistema informático posee vulnerabilidades se podrá generar un ataque para generar un impacto sobre él y hasta tomar control de este. Los ataques pueden ser tanto intencionales como fortuitos, pero de igual forma puede poner en riesgo un sistema, un ataque informático pasa por las siguientes fases según (Gascó, Serrano, & Ramada, 2013):

- **Reconocimiento**, obtiene toda la información necesaria de la víctima, sea una persona o una organización.
- **Exploración**, obtener información sobre el sistema a atacar, pueden ser direcciones IP, nombres de host, etc.
- **Obtención de acceso**, con la información obtenida, se intenta explotar las vulnerabilidades detectadas.
- **Mantener el acceso**, una vez accedido al sistema, se buscará la forma de implementar herramientas que permitan el acceso nuevamente en futuras ocasiones.
- **Borrar las huellas,** por último, se intentará borrar las huellas que se hayan dejado durante la intromisión para evitar ser detectado.

4.4.2.6. Impactos

Son las consecuencias de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

4.4.3. Seguridad de Sistemas de Información

Según (Aguilera, 2010) para implementar una política de seguridad en un sistema de información es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.

- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección.

4.4.4. Metodologías de análisis de riesgos

"Dado que los riesgos no tienen el mismo origen ni la misma naturaleza, existen varias estrategias para su gestión. Sin embargo, otros factores que indicen significativamente son el tamaño de las empresas, su número de integrantes, su estructura, la actividad de producción y el sector en el que operan." (Jhuéz, 2018)

Debido a lo mencionado anteriormente se han desarrollado algunas metodologías de análisis propias de cada especialidad, las mismas que tienen como objetivo identificar, evaluar, tratar y monitorizar los riesgos que están asociados a una actividad o proceso, a pesar de esto se deja en claro que existen dos grupos principales de metodologías:

4.4.5. Metodologías de gestión de riesgo

Según (Jhuéz, 2018) son aquellas que están orientadas a identificar, evaluar y posterior tratamiento de los riesgos derivados de una actividad. Entre las más conocidas están:

- Norma ISO 31000
- Norma AS/NSZ
- Sistema APPCC
- Método ARO

4.4.6. Metodologías de cuantificación

Según (Jhuéz, 2018) trata de aquellas herramientas que se enfocan exclusivamente en la cuantificación de riesgos. Es decir, aplican una serie de indicadores (de carácter numérico casi siempre) para medir el impacto que tienen los riesgos en las organizaciones y, a partir de ese cálculo, elaborar acciones coordinada para su gestión, tratamiento o, incluso, eliminación.

En la Tabla 3 se observa la comparación entre las metodologías de análisis y gestión de riesgos que son de uso habitual para seguridad de la información, con la

misma que se determinará cuál es la metodología que genere más confianza en la mitigación de riesgos.

Tabla 4. Comparación de metodologías.

		MAGERIT	OCTAVE	CRAMM	IRAM
Alcance considerado	**Análisis de Riesgos**	100%	100%	100%	100%
	Gestión de Riesgos	100%	100%	100%	100%
Tipo de Análisis	**Cuantitativo**	100%	50%	100%	100%
	Cualitativo	100%	50%	100%	100%
	Mixto	100%	50%	0%	0%
Tipo de Riesgos	**Intrínseco**	100%	0%	100%	100%
	Efectivo	100%	100%	100%	100%
	Residual	100%	25%	0%	25%
Elementos del modelo	**Procesos**	100%	100%	0%	0%
	Activos	100%	100%	100%	100%
	Recursos	100%	100%	0%	0%
	Dependencias	100%	100%	100%	100%
	Vulnerabilidades	100%	100%	100%	100%
	Amenazas	100%	100%	100%	100%
	Salvaguardas	75%	100%	100%	100%
Objetivos de seguridad	**Confidencialidad**	100%	100%	100%	100%
	Integridad	100%	100%	100%	100%
	Disponibilidad	100%	100%	100%	100%
	Autenticidad	100%	0%	0%	0%
	Trazabilidad	100%	0%	0%	0%
Inventarios	**Tipo de Recursos**	100%	100%	100%	0%
	Vulnerabilidades	100%	100%	100%	100%
	Amenazas	100%	100%	100%	100%
	Salvaguardas	100%	100%	0%	100%
Ayudas a la implantación	**Herramienta**	100%	0%	100%	100%
	Plan de Proyecto	100%	100%	25%	0%
	Técnicas	100%	100%	0%	0%
	Roles	100%	100%	100%	0%
	Comparativas	100%	0%	100%	0%
	Otros	0%	Cuestionarios	Cuestionarios	Soporte ISF

Obtenido de: (Álvarez, 2014)

4.4.7. Herramientas para escaneo de vulnerabilidades

Para llevar a cabo el análisis de vulnerabilidades que afectan a los activos de la institución se realizó una comparación entre algunos softwares que tiene la función de escáneres de vulnerabilidades, de los cuales se escogerá uno.

Tabla 5. Comparación de Software para escaneo de vulnerabilidades

	Qualysguard	**Rapid7**	**NESSUS**
Tipo de Interfaz	Interfaz obsoleta en ventanas emergentes que entorpece la configuración.	Diseño de tableros poco intuitivos que se cargan en la nube.	Simple, concreta y orientada al uso con plantillas predefinidas basadas en SCADA.
Configuración	Admite únicamente direcciones IP.	Requiere creación previa de políticas y credenciales por separado.	Viene con políticas precargadas que luego pueden redefinirse.
Despliegue de escaneo	Demanda de configuración previa de políticas de funcionamiento.	Necesita configuración previa para ejecutar escaneo.	Plugins precargados para realizar escaneos.
Tiempo para finalizar escaneo	No existen datos.	Dos horas.	Depende el rango.
Modelo de escaneo	Cuenta con agente configurado totalmente desde la nube, lo cual consume bastante ancho de banda.	Integra agente para monitoreo.	Cuenta con agentes para dispositivos móviles.
Tipo de servicio	Solución SaaS que deja por fuera servicios bajo modelo On-Premise.	Escáner activo.	Escaneo activo que se integra con servicio de escaneo pasivo (PVS).
Políticas	Necesitan ser configuradas antes del inicio del servicio, lo que entorpece el resultado.	Configuración limitada para la creación de políticas de auditoría.	Cuenta con políticas para análisis de malware que opera en conjunto con antivirus.
Aspectos adicionales	Carece de opción para escaneo de vulnerabilidades a través de MDM.	No ofrece soporte o documentación para detección malware.	Ejecuta análisis de vulnerabilidades a través de MDM.

Elaborado por: Los autores

Comparando los puntos en la tabla anterior se puede concluir que la herramienta que conveniente para el respectivo análisis es NESSUS, por la facilidad en instalación, configuración y puesta en marcha de este.

4.5. Seguridad Perimetral

"La seguridad perimetral se basa en proteger a todo el sistema informático de una empresa desde "fuera" es decir, implementar una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para la red." (Rabadán, 2008)

4.5.1. Objetivos de la seguridad perimetral

Implementar un sistema de seguridad perimetral beneficia al momento de proteger la red tanto de ataques internos como externos, para ello se han planteado objetivos que debe cumplir el sistema:

- Proporciona mayor productividad a los usuarios, permitiendo acceder a sitios seguros y además que se asocien al ambiente laboral y no al entretenimiento.
- Protección a los equipos de red ya que la mayoría de las amenazas provienen de internet, debido a la interacción de los usuarios con el mismo.
- Detección de virus y programas maliciosos.
- Optimizar el uso del internet para los usuarios de la red, administrando la capacidad y velocidad dependiendo del rol que desempeñen.

4.5.2. Requisitos de la seguridad perimetral

Según (Londoño, 2014). "Una técnica de seguridad informática es un mecanismo o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático", por lo tanto, se deben cumplir los siguientes requisitos adicional a los que menciona la cita:

- **Identificación, e**s la verificación que se realiza al momento en que el usuario se da a conocer en el sistema.
- **Autentificación, e**s la verificación de que el usuario que se ha identificado en el sistema es seguro.

- **Control de acceso**, es la administración correcta de los usuarios que acceden a la red, mientras que a los usuarios seguros se les da el acceso necesario, a los usuarios maliciosos se les deniega el acceso.
- **Confidencialidad**, es la protección de la información que los usuarios seguros tienen dentro de la red ante los usuarios no autorizados.
- **Integridad**, es la protección de datos y transmisiones contra las alteraciones no autorizadas o accidentales que pueden ocurrir dentro de la red.
- **Responsabilidad**, es realizar el seguimiento y almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red, tanto por los usuarios seguros como usuarios maliciosos.

4.5.3. UTM (Unified Threat Management)

Según (Cameron, Woodberg, Giecco, Eberhard, & Quinn, 2010) un Gestor Unificado de Amenazas es un conjunto de funcionalidades diseñadas para proporcionar la inspección del tráfico que cruza por la red en la capa de aplicación. Similar a la detección y prevención de intrusiones, los dispositivos de seguridad que soportan funciones UTM descifran e inspeccionan los protocolos en la capa superior para detectar tráfico malicioso o desconocido.

Las características de un Gestor Unificado de Amenazas son:

- Funciones de firewall
- Filtrar correo
- Antispam
- Detección y bloqueo de malware
- Filtrar contenido WEB
- Prevención y detección de intrusos
- Soporte de VPN y SSL

4.6. Directorio Activo

El directorio activo es una herramienta proporcionada por Microsoft que sirve para la organización y gestión de los recursos de una red y todo lo que ello implica: usuarios, servicios, puestos, impresoras permisos, servidores, etc.

Según (Molina & Baena, 2007), el Directorio Activo es un servicio de directorio que almacena información acerca de los objetos de una red y la pone a

disposición de los usuarios y administradores de la red. Permite controlar desde un solo servidor todos los equipos de la red, sin tener que desplazarse a los equipos clientes.

Cuando no se cuenta con servidor de directorio activo y se administra muchos equipos, se tendrá que movilizar a cada equipo para configurar su entorno y los usuarios que pueden usarlo. Mientras que con el Directorio Activo esta tarea se realiza exclusivamente desde el servidor. Se crean usuarios, perfiles, restricciones, etc.

4.6.1. Estructura del Directorio Activo

Según (Trejos S., 2013), la estructura lógica del Directorio se centra en la administración de los recursos de la organización, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes. La estructura lógica de la organización se basa en el concepto de dominio, o unidad mínima de directorio, que internamente contiene información sobre los recursos (usuarios, grupos, computadores, directivas, etc.) existentes en dicho dominio.

Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de unidades organizativas, que permiten una administración independiente sin la necesidad de crear múltiples dominios. Sin embargo, si la organización necesita estructurarse en varios dominios, también puede hacerlo, mediante los conceptos de árbol y bosque; ambos son jerarquías de dominios a distintos niveles, en función de si los dominios comparten o no un espacio de nombres común. (p. 9)

4.6.1.1. Estructura lógica

Dicha estructura se encarga de administrar los recursos de red sin tomar en cuenta su ubicación física, ni las topologías de redes. La estructura lógica posee componentes que serán detallados a continuación.

- **Objetos. –** Es el nombre que representará a cada recurso de la red. Los objetos poseen atributos que son las características de cada uno.

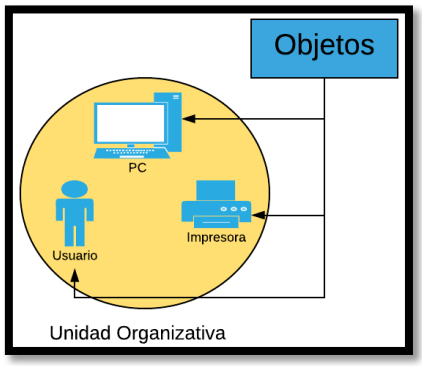


Figura 4. Objetos
Obtenido de: (Molina & Baena, 2007)

- **Unidades Organizativas.** - Es donde los objetos se encuentran alojados, sirven para tener una mejor administración de los objetos, a estos se les puede delegar políticas de dominio para tener diferentes configuraciones sobre los tipos de objetos que estén dentro de la misma.

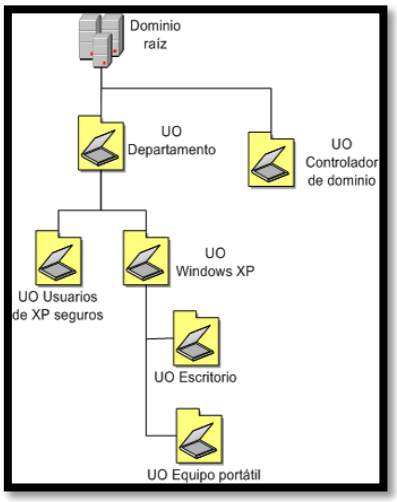


Figura 5. Unidades Organizativas
Obtenido de: (Microsoft, 2006)

- **Dominios.** – Es la unidad central de la estructura, los mismos son definidos por el administrador de la red, están agrupados por el mismo nombre, los dominios son controlados por el controlador de dominio.
- **Árbol de dominio.** – Dominios agrupados de forma jerárquica.
- **Bosque.** – El conjunto de árboles de dominio.

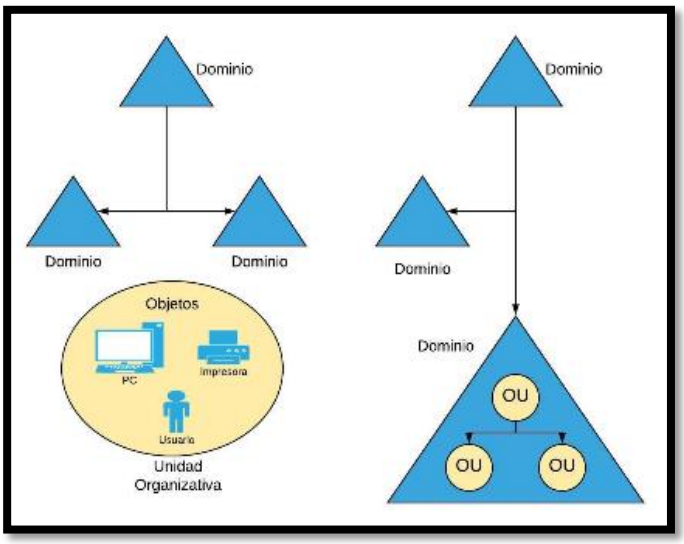


Figura 6. Estructura lógica
Elaborado por: Los autores

4.7. Normas ANSI/TIA/EIA 606-A

La norma ANSI/TIA/EIA 606-A especifica la administración para sistemas de cableado de telecomunicaciones. Proporciona un enfoque de administración que no depende de las aplicaciones, ya que la mismas pueden cambiar. Establece las directrices para todos los participantes de la administración de la infraestructura de telecomunicaciones, desde el usuario final hasta los instaladores de la red.

4.7.1. Clases de administración

Según (ANSI/TIA, 2002) la norma determina cuatro clases de administración, las cuales dependen del tamaño de la red y ciertas características de la infraestructura de telecomunicaciones.

Clase 1

Es utilizada para sistemas que están en un solo edificio con una sala de telecomunicaciones. La sala de telecomunicaciones, los enlaces horizontales y la puesta a tierra deben etiquetarse y administrarse.

Clase 2

Está dirigida a sistemas que están en un solo edificio, pero con más de una sala de telecomunicaciones, en esta clase se incluirán puntos de seguridad contra incendios y varios elementos del sistema puesta a tierra.

Clase 3

La clase 3 está orientada a sistemas que constan varios edificios, es más conocida como "Entorno de campus". En esta clase se incluye la administración para edificios y el cableado entre edificios, así mismo todos los elementos de clase 2.

Clase 4

La clase 4 está dirigida a sistemas conformados por varios campus, en esta clase se incluye la administración de cada sitio, así como los elementos de clase 3 y se recomienda identificar el cableado "inter - campus", como son las conexiones tipo MAN o WAN.

4.8. Metodología

La metodología que se utilizará para el presente proyecto consta de 4 fases que se detallan a continuación:

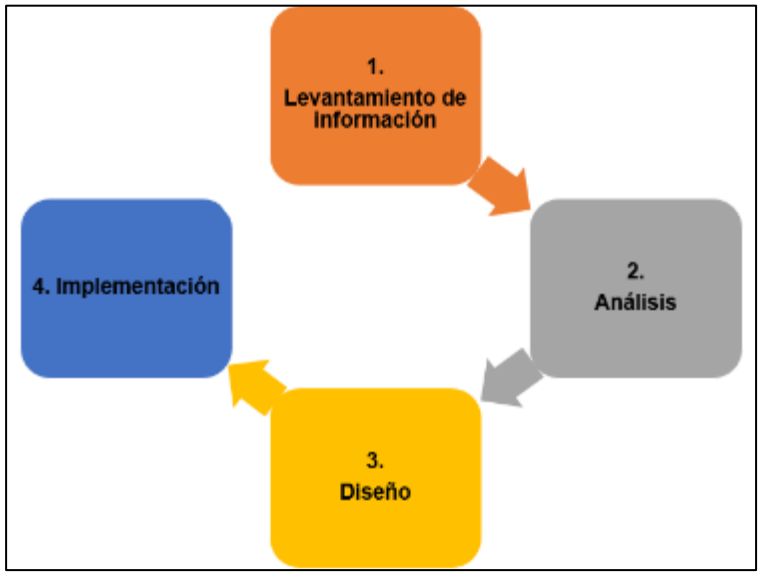


Figura 7. Fases de metodología
Elaborado por: Los autores

4.8.1. Levantamiento de Información

En esta fase se procederá a realizar un listado de tareas como lo son: entrevista con el personal del departamento correspondiente, encuesta de satisfacción a los funcionarios públicos de la Gobernación del Guayas con respecto al estado actual de la red y el servicio de internet, así como identificación de los equipos, servicios y su interacción con la red de datos interna, con el fin de conocer las deficiencias y necesidades que posee esta institución gubernamental. Se culminará con la entrevista

al responsable del área de Tecnología de la Información y Comunicación para comunicar y proceder de forma objetiva y profesional con las fases siguientes de Análisis, Diseño y la respectiva Implementación.

4.8.2. Análisis

Basados en la información recopilada en la fase anterior, se continuará con el examen detallado de los equipos y servicios detallados, para conocer sus características y estado para con ello, proceder con la extracción de conclusiones necesarias para el diseño de la solución.

4.8.3. Diseño

Utilizando los requisitos técnicos planteados y verificados de acuerdo con el análisis, se continuará con el planteamiento del diseño de solución donde se determinará las características a detalle de se requieren para la implementación en hardware y software en cumplimiento de los objetivos planificados.

4.8.4. Implementación

De acuerdo con el diseño detallado, se procederá a la ejecución de este. Se comenzará con la instalación, configuración e integración del software que se determinó como solución a los requerimientos de la institución para mitigar el impacto de ataques a las vulnerabilidades a la red interna; así como el plan de reestructuración de direccionamiento IP y aplicación de las normas ANSI/TIA/EIA 606A.

5. Marco Metodológico

5.1. Levantamiento de información

Para iniciar esta fase se realizó el análisis de la situación actual en la institución, mismo que se realizó manteniendo una reunión con el responsable de la Unidad de Tecnología de la Información y Comunicación, siendo el encargado de administrar y gestionar la red de activos informáticos dentro de la Gobernación del Guayas y realizando una encuesta a los servidores públicos que laboran en el edificio de Planta Central.

El personal de Tecnología conoce la realidad de la institución en cuanto a la seguridad de la información que manejan y la identificación de los activos de la red y su respectiva organización y administración.

Una vez comprendido el estado actual de la red se procedió a realizar el levantamiento de información de todos los activos, actualizando reportes y elaborando planos de cada piso y departamento con sus respectivos equipos y puntos de datos, los mismos con los que no contaba el departamento y los cuales beneficiarán tanto a la institución como a los autores del presente proyecto.

En esta etapa se concluyó que la institución cuenta con infraestructura de la cual la Unidad de TIC's es responsable, motivo por el que este proyecto se llevará a cabo con apoyo del personal de esta área.

5.1.1. Entrevista con el responsable de la Unidad de TIC's

Con el fin de obtener información técnica acerca de las necesidades de la institución con respecto a equipos y servicios internos, se procedió a agendar una entrevista con el responsable de la Unidad de Tecnología, misma que permitió encontrar los puntos a solucionar dentro del proyecto, los cuales se detallan a continuación:

- No existe ninguna documentación sobre el cableado estructurado.
- Desorganización de la distribución IP.
- Ausencia de esquemas de seguridad en la red.
- Computadoras interconectadas dentro de grupo de trabajo.

El detalle de las preguntas realizadas en la entrevista se encuentra en el **Anexo A.**

5.1.2. Encuesta a los funcionarios públicos

Con el objetivo de conocer el nivel de satisfacción de los funcionarios públicos que laboran en el edificio de Planta Central de la Gobernación del Guayas con respecto a los servicios de red e internet que usan en la actualidad, se procedió a crear una encuesta con las interrogantes detalladas, y de las cuales se obtuvieron porcentajes que están detallados en el **Anexo B** y a continuación serán analizados:

1.- Fácil acceso a páginas institucionales:

La satisfacción de los usuarios de la red interna con respecto al acceso a páginas institucionales es notablemente baja, teniendo en cuenta que los niveles de satisfacción fueron los siguientes: Con el 12.5% para muy satisfecho, 25% satisfecho, 15.6% poco satisfecho, 25% insatisfecho, 15.6% es indiferente y el 6.3% no utiliza las páginas. Se puede decir que esto se debe a que el tráfico de la red no está correctamente distribuido, lo que conlleva a que dichas webs no funcionen con normalidad.

2.- Velocidad de Internet:

Sobre la velocidad de navegación por internet para los usuarios de la red de internet es demasiado bajo, teniendo en cuenta que los niveles de satisfacción fueron los siguientes: Con el 12.5% para muy satisfecho, 18.8% satisfecho, 28.1% poco satisfecho, 21.9% insatisfecho, 12.5% es indiferente y el 6.2% no tiene conocimiento al respecto. Se puede decir que esto se debe a que no se está realizando un correcto filtrado de accesos a internet y distribución del ancho de banda.

3.- Seguridad en navegación web:

Los usuarios de la red interna tienen un bajo nivel de satisfacción con respecto a la seguridad de navegación web teniendo en cuenta que el 12.5% está muy satisfecho, el 12.5% satisfecho, el 28.1% poco satisfecho, el 28.1% insatisfecho, el 12.5% es indiferente y el 6.3% no hace uso de la navegación web. Estos niveles de insatisfacción se deben a falta de conocimiento y experiencia con equipos infectados por virus de manera habitual.

4.- Seguridad de correo institucional:

Con respecto a la seguridad del correo institucional los usuarios han dado a notar claramente que se encuentran insatisfechos, ya que solo el 3.15% está muy satisfecho, el 25% satisfecho, el 21.9% poco satisfecho, el 34.4% está insatisfecho, el 12.5% es indiferente al respecto y el 3.15% no utiliza correo institucional. Se puede decir que la mayoría de los usuarios está recibiendo demasiado spam y correo basura.

5.- Seguridad de la Información:

De la seguridad de la información se puede decir que los usuarios están insatisfechos porque solo el 3.1% se encuentra muy satisfecho con la misma, el 15.6% está satisfecho, el 21.9% está poco satisfecho, el 37.5% insatisfecho, el 18.8% es indiferente y el 3.1% no tiene acceso a información, esto se debe a la falta de seguridad en la red interna ya que los equipos no poseen ningún sistema de seguridad.

6.- Servicio de Internet:

Los usuarios de la red interna indican que están insatisfechos con el servicio de internet, teniendo en cuenta que solo el 3.1% está muy satisfecho, el 31.3% satisfecho, el 25% poco satisfecho, el 28.1% insatisfecho, el 9.4% es indiferente y el 3.1% no lo utiliza. Se puede asumir que esto se debe a que presentan varias perdidas de paquetes y largas jornadas sin acceso a internet.

5.1.3. Esquema de topología de red

El esquema actual de topología de red está dividido en dos partes: física y lógica especificada de la siguiente manera:

5.1.3.1. Topología lógica

La topología lógica de la Gobernación del Guayas es tipo bus Ethernet, ya que todos los dispositivos se encuentran conectados por un mismo medio.

Los equipos se comunican entre sí mediante conexiones de cable de red categoría 6, conexiones de 10/100 en puertos finales y 10/100/1000 para conexiones entre switches; lo cual permite la interconexión entre los diferentes equipos que conforman la red.

5.1.3.2. Topología física

La topología física de la Gobernación del Guayas es tipo estrella extendida, debido a que los switches se encuentran conectados al nodo central.

En la figura 8, se visualiza la topología física que se encuentra actualmente implementada en la Gobernación del Guayas.

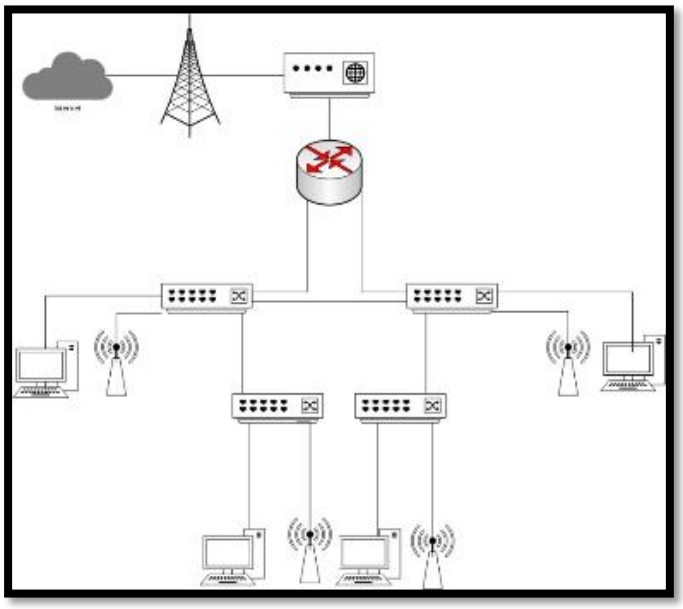


Figura 8. Topología física
Elaborado por: Los autores

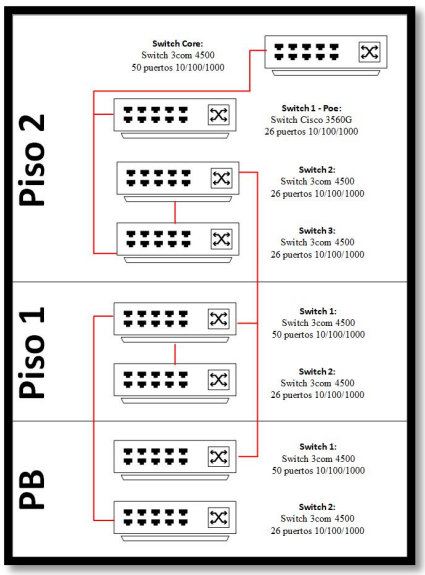


Figura 9. Interconexión de switches por piso
Elaborado por: Los autores

5.1.4. Racks del edificio

En la siguiente descripción se detalla los Racks que se encuentran distribuidos alrededor de todo el edificio de Planta Central de la Gobernación del Guayas.

En la Figura 10, se visualiza el Rack del Data Center con los cables desorganizado y algunos de ellos no se encuentran conectados a ningún switch, y nadie tiene conocimiento de estos debido a la falta de etiquetado y documentación del cableado.

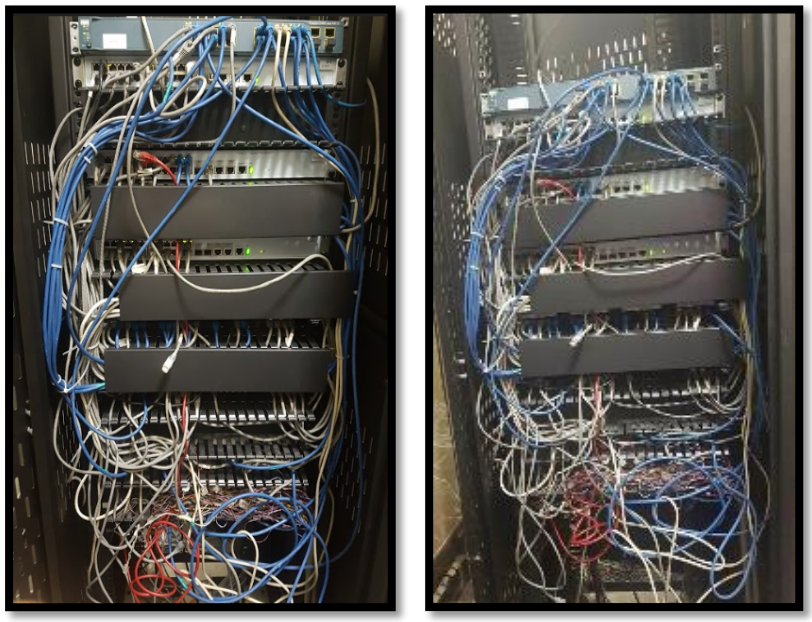


Figura 10. Rack de Segundo Piso
Elaborado por: Los autores

En la Figura 11. Rack de Servidores, se visualiza el Rack de Servidores ubicado en el Data Center, en el cual se encuentran servidores que están funcionando y otros que han dejado de funcionar, pero no han sido dados de baja.

Figura 11. Rack de Servidores
Elaborado por: Los autores

Los Racks identificados en las Figuras 10 y 11 se encuentran ubicados en el segundo piso del edificio.

En la Figura 12, se visualiza el Rack ubicado en el primer piso donde se distribuye el acceso a la red para los usuarios de ese piso.

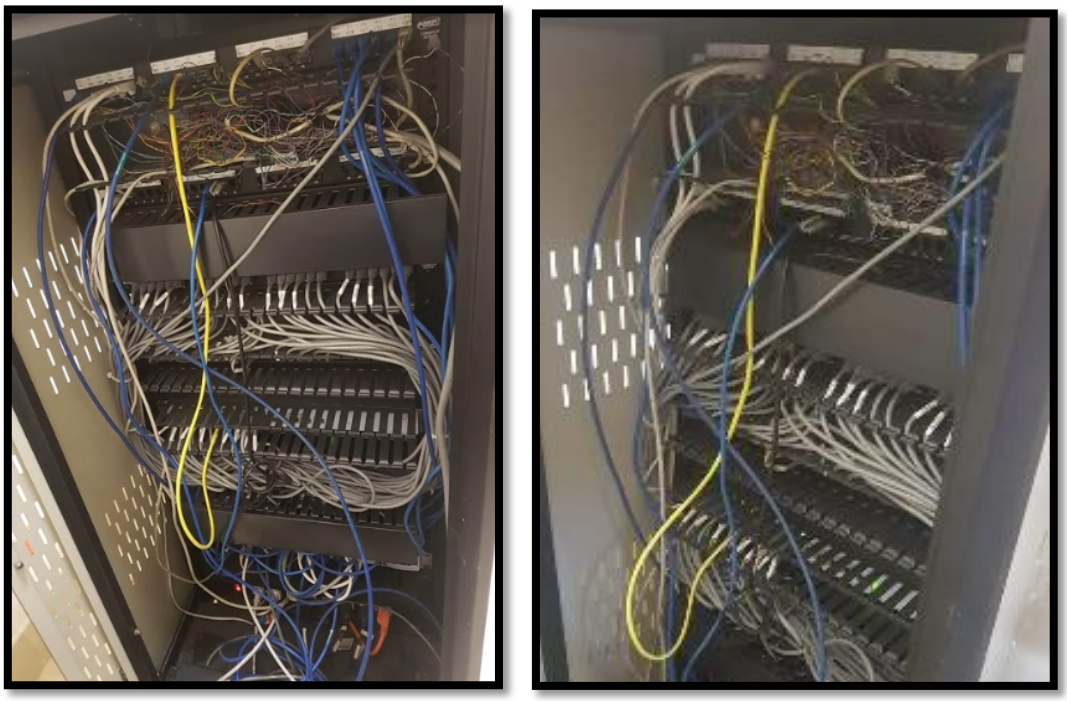


Figura 12. Rack de primer piso
Elaborado por: Los autores

En la Figura 13 y 14, se visualiza los Rack 1 y 2 respectivamente, ubicados en la planta baja, los mismos que distribuyen el acceso a la red para los usuarios en ese piso.

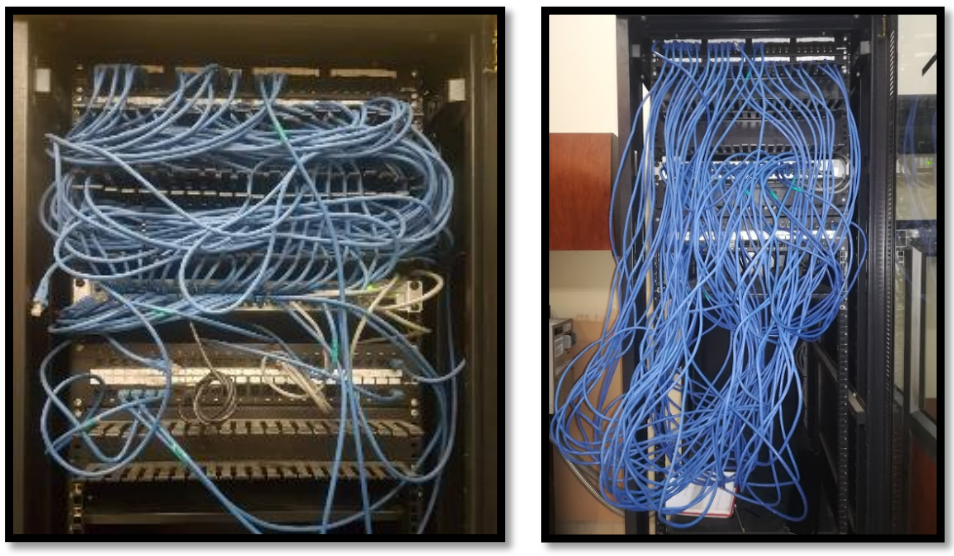


Figura 13. Rack 1 de planta baja
Elaborado por: Los autores

Figura 14 Rack 2 de planta baja
Elaborado por: Los autores

Como factor común en cada Rack descrito anteriormente se denota que:

- Existen cables de red desconectados.
- Existen cables conectados de una central telefónica que ya no está en uso.
- No existe etiquetado que facilite el reconocimiento de puntos.

5.1.5. Planos del edificio

Para el levantamiento de los puntos de red existentes, se elaboraron los planos de: Planta Baja, Primer y Segundo piso respectivamente, así como de cada uno de los departamentos, utilizando la herramienta Microsoft Visio:

Cabe detallar que, de acuerdo con la antigua clasificación de puntos, éstos fueron divididos y representados de la siguiente forma:

Tabla 6. Representación de puntos de voz y datos.

Punto de acceso	Representación
Punto de Datos	
Punto de Voz	

Elaborado por: Los autores

5.1.5.1. Planta baja

En la Figura 14, se puede visualizar el plano correspondiente a la planta baja con la respectiva ubicación de los puntos de red.

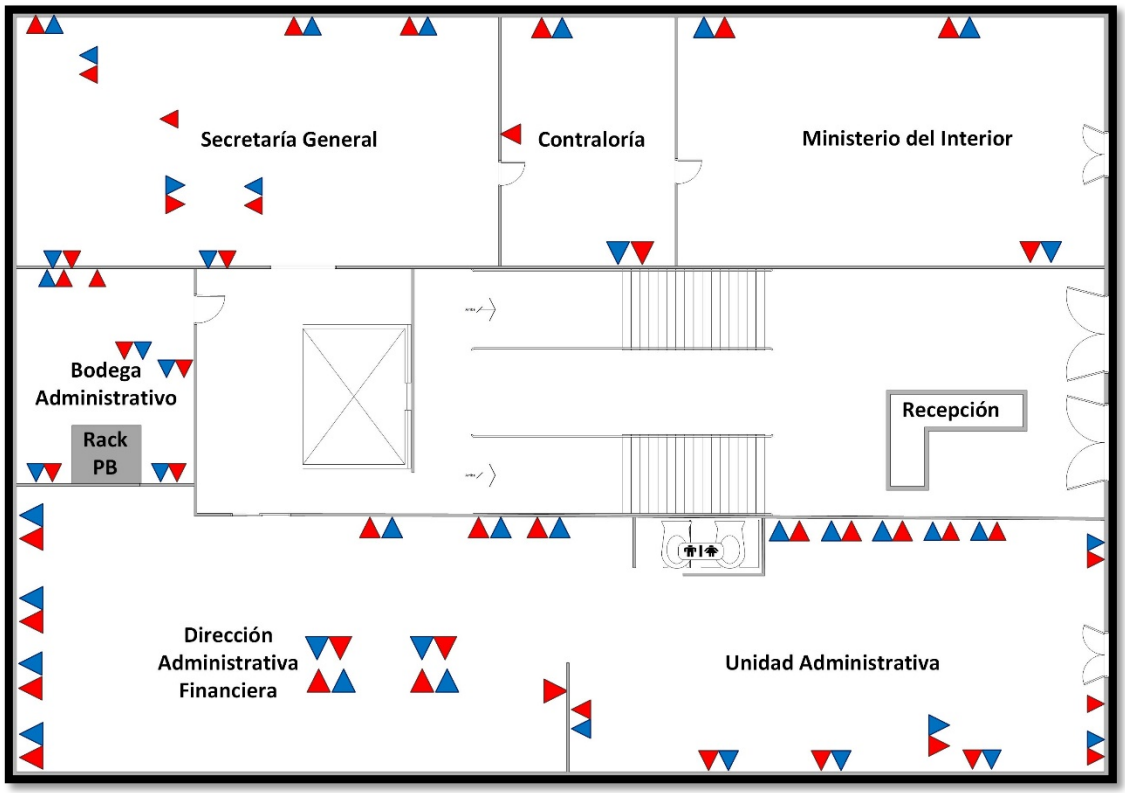


Figura 15. Planos de planta baja
Elaborado por: Los autores

Para una mejor apreciación, en la Tabla 11 se detalla los puntos de red por departamentos que se encuentran en la planta baja.

Tabla 7. Puntos de red en planta baja.

Departamentos	Puntos de red
Unidad Administrativa	25
Bodega Administrativo	11
Ministerio del Interior	6
Dirección Administrativa Financiera y Unidad Financiera	23
Secretaría General	17
Contraloría	5
Recepción	1

Elaborado por: Los autores

5.1.5.2. Primer piso

En la Figura 15, se puede visualizar el plano correspondiente al primer piso con la respectiva ubicación de los puntos de red.

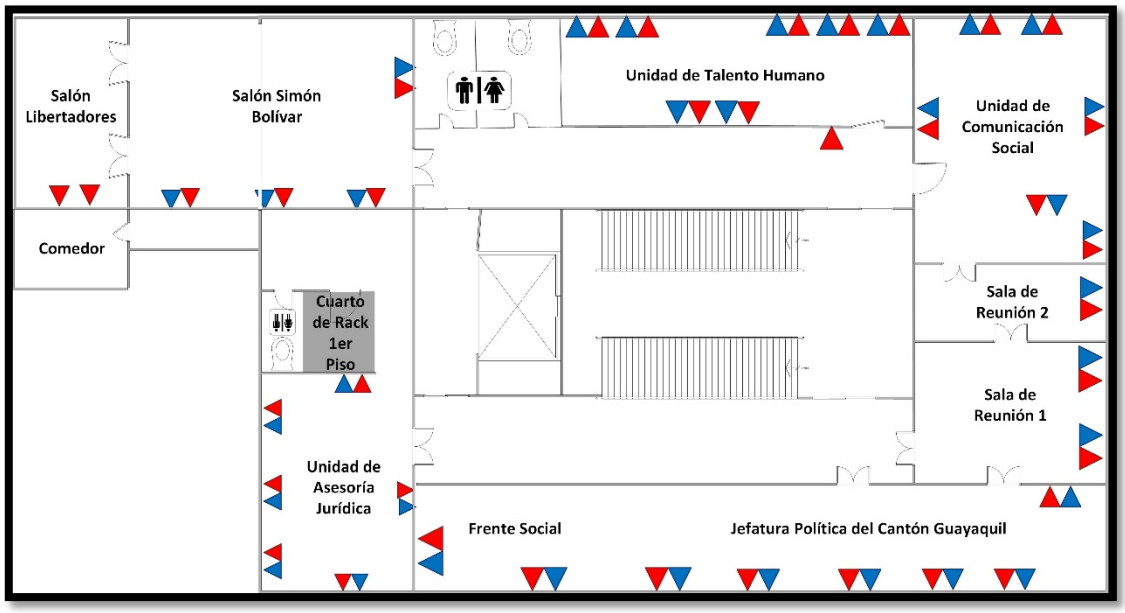


Figura 16. Planos del primer piso
Elaborado por: Los autores

Para una mejor apreciación, en la Tabla 8 se detalla los puntos de red por departamentos que se encuentran en el primer piso.

Tabla 8. Puntos de red en primer piso

Departamentos	Puntos de red
Unidad de Comunicación Social	12
Sala de Reuniones 1	4
Sala de Reuniones 2	2
Jefatura Política del Cantón Guayaquil	12
Frente Social	4
Unidad de Asesoría Jurídica	12
Unidad Administrativa de Talento Humano	15
Salón Simón Bolívar y Salón Libertadores	10

Elaborado por: Los autores

5.1.5.3. Segundo piso

En la Figura 16, se puede visualizar el plano correspondiente al segundo piso con la respectiva ubicación de los puntos de red.

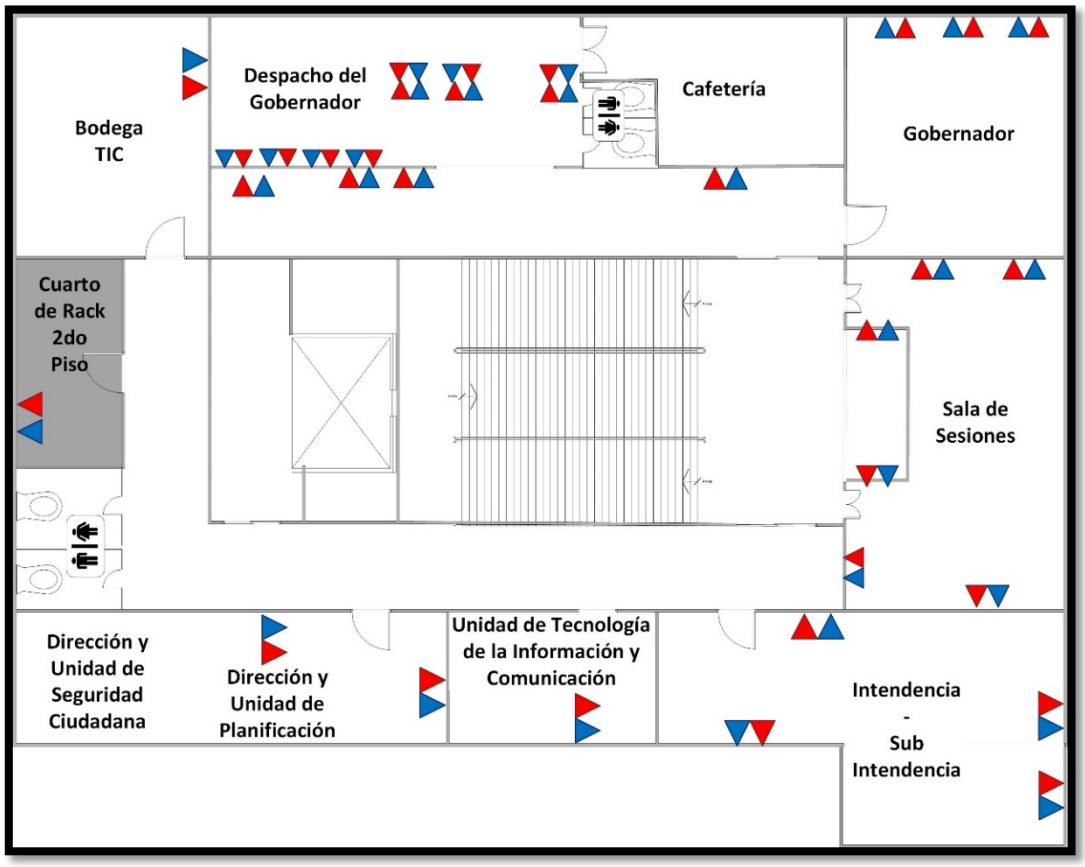


Figura 17. Planos del segundo piso
Elaborado por: Los autores

Para una mejor apreciación, en la Tabla 9 se detalla los puntos de red por departamentos que se encuentran en segundo piso.

Tabla 9. Puntos de red del segundo piso

Departamentos	Puntos de red
Despacho del Gobernador	34
Bodega de TIC	2
Dirección de Planificación y Unidad de Planificación e Inversión	2
Dirección de Seguridad Ciudadana y Unidad de Seguridad Ciudadana	2
Unidad de Tecnología de la Información y comunicación	2
Intendencia – Sub Intendencia	8
Sala de sesiones	12

Elaborado por: Los autores

5.1.6. Direccionamiento IP

En la Tabla 9 se detalla las IP, departamento y usuario o equipo a los cuales han sido asignadas. Cabe recalcar que, de acuerdo con la información recibida por

el personal de la Unidad de Tecnología, conforme a la necesidad inmediata de la asignación de una dirección IP a un equipo, el departamento una vez utilizadas las IP's de en el orden de la tabla adjunta, proceden a fijar una dirección disponible de otro departamento, por lo que la información del cuadro varía:

Tabla 10. Distribución IP por departamento.

Distribución IP		
Departamento	**Dirección IP**	**Asignación**
Tecnología y comunicación	192.168.2.1 - 192.168.2.7	Servidores
	192.168.2.12	Biométrico
	192.168.2.21 - 192.168.2.26	Usuarios
	192.168.2.27 - 192.168.2.29	Reservadas
	192.168.2.20	Impresora
Despacho del Gobernador	192.168.2.31 - 192.168.2.35	Usuarios
	192.168.2.36 - 192.168.2.39	Reservadas
	192.168.2.30	Impresora
Comunicación	192.168.2.41 - 192.168.2.52	Usuarios
	192.168.2.52 - 192.168.2.59	Reservadas
	192.168.2.40	Impresora
Unidad administrativa	192.168.2.61 - 192.168.2.68	Usuarios
	192.168.2.69	Reservada
	192.168.2.60	Impresora
Dirección financiera	192.168.2.71 - 192.168.2.78	Usuarios
	192.168.2.79	Reservada
	192.168.2.70	Impresora
Secretaría General	192.168.2.81 - 192.168.2.88	Usuarios
	192.168.2.89	Reservada
	192.168.2.80	Impresora
Jurídico	192.168.2.91 - 192.168.2.95	Usuarios
	192.168.2.96 - 192.168.2.99	Reservadas
	192.168.2.90	Impresora
Jefatura Política	192.168.2.101 - 192.168.2.108	Usuarios
	192.168.2.109	Reservada

	192.168.2.100	Impresora
Talento Humano	192.168.2.111 - 192.168.2.118	Usuarios
	192.168.2.119	Reservada
	192.168.2.110	Impresora
Unidad de Planificación	192.168.2.121 - 192.168.2.126	Usuarios
	192.168.2.127 - 192.168.2.129	Reservadas
	192.168.2.120	Impresora
Frente Social	192.168.2.131 - 192.168.2.136	Usuarios
	192.168.2.137 - 192.168.2.139	Reservadas
	192.168.2.130	Impresora
Seguridad Ciudadana	192.168.2.141 - 192.168.2.148	Usuarios
	192.168.2.149	Reservada
	192.168.2.140	Impresora
Ministerio del Interior y Contraloría	192.168.2.151 - 192.168.2.153	Usuarios

Elaborado por: Los autores

La Gobernación de la Provincia del Guayas, al momento se encuentra utilizando tres redes LAN:

- Red 192.168.1.0 donde se encuentran configurados los equipos: Switches y Access Point.
- Red 192.168.2.0 donde se encuentran los equipos de Usuarios, Servidores e Impresoras.
- Red 192.168.3.0 donde se encuentra la Central Telefonica IP Asterisk.

5.2. Análisis

5.2.1. Análisis de riesgos de la seguridad de la red: Metodología MAGERIT

De la tabla 3 desarrollada en los Fundamentos teóricos se puede concluir que MAGERIT es la metodología que cumple al 100% todos los campos.

MAGERIT se basa en analizar el impacto que puede tener para la empresa, identificando las amenazas que pueden afectar y las vulnerabilidades que puedan ser

utilizadas por las mismas, de esta manera se logrará tener una correcta identificación de las medidas preventivas y correctivas. También se tomará en cuenta que debido a que la empresa recién inicia en su labor de gestión de la seguridad de la información, la metodología es la más indicada, dado que, permite enfocar los esfuerzos en los riesgos que serán críticos.

Con el análisis de riesgos se analizará los elementos metódicamente y llegar a conclusiones con fundamento. Para este proceso de análisis se realizarán los siguientes pasos:

5.2.1.1. Identificación y clasificación de activos de la red

Identificar los activos de la red es importante ya que permite valorar de forma exacta e identificando y valorando las amenazas a las que están expuestos dichos activos. Se realizó la respectiva recolección de información de los activos.

Planta baja

En la Tabla 11, se detallarán marcas, descripciones y estados de los equipos existentes en la planta baja.

Tabla 11. Activos en planta baja.

Cantidad	Equipo	Descripción	Estado
1	Switch 3com 4500	26 puertos 10/1000/1000	Operativo
1	Switch 3com 4500	50 puertos 10/1000/1000	Operativo
2	AP Cisco	Aironet 1130	Operativo

Elaborado por: Los autores

En la Tabla 12, se detalla cuántos usuarios de red hay en planta baja y los respectivos departamentos.

Tabla 12. Cantidad de usuarios en planta baja.

Departamentos	Usuarios
Contraloría	33 aproximadamente
Dirección Administrativa Financiera	
Secretaria General	
Recepción	
Unidad Administrativa	
Ministerio del Interior	

Elaborado por: Los autores

Primer piso

En la Tabla 13, se detallarán marcas, descripciones y estados de los equipos existentes en el primer piso.

Tabla 13. Activos en primer piso.

Cantidad	Equipo	Descripción	Estado
1	Servidor Xtratech	Antivirus Kaspersky	No funciona
1	Servidor HP Pro 3130	ANASAFi	No funciona
1	Switch 3com 4500	26 puertos 10/100/100	Operativo
1	Switch 3com 4500	50 puertos 10/100/100	Operativo
1	AP Cisco	Aironet 1130	Operativo

Elaborado por: Los autores

En la Tabla 14, se detalla cuántos usuarios de red hay en primer piso y los respectivos departamentos.

Tabla 14. Cantidad de usuarios en primer piso.

Departamentos	Usuarios
Unidad de Comunicación Social	40 aproximadamente
Unidad de Talento Humano	
Jefatura Política del Cantón Guayaquil	
Unidad de Asesoría Jurídica	
Frente Social	

Elaborado por: Los autores

Segundo piso

En la Tabla 15, se detallarán marcas, descripciones y estados de los equipos existentes en el segundo piso.

Tabla 15. Activos en segundo piso.

Cantidad	Equipo	Descripción	Estado
2	Switch 3com 4500	26 puertos 10/100/1000	Operativo
1	Switch 3com 4500	50 puertos 10/100/1000	Operativo
1	Switch Cisco 3560G	26 puertos 10/100/1000	Operativo
2	Servidor HP DL 120 G6	Servidor de archivos	No funciona
		Sin S.O.	No funciona

3	IBM X3650 M3	Servidor de archivos y SQL	Operativo
		SASIC	No funciona
		Sin S.O.	No funciona
2	HP ML350 G8	VMWARE ESXI 5,1	Operativo
		Zimbra	Operativo
1	DELL Optiplex 990	Central AsterCC	No funciona
1	Genérico	Central AsterCC	Operativo
2	AP Cisco	Aironet 1130	Operativo

Elaborado por: Los autores

En la Tabla 16, detallamos cuántos usuarios de red hay en segundo piso y los respectivos departamentos.

Tabla 16. Cantidad de usuarios en segundo piso.

Departamentos	Usuarios
Despacho del Gobernador	20 aproximadamente
Dirección de Planificación e Inversión	
Unidad de Tecnología de la Información y comunicación	
Intendencia – Sub Intendencia	
Dirección de Seguridad Ciudadana	

Elaborado por: Los autores

5.2.1.1.1. Valoración de los activos

Mediante la identificación de activos se define que, los activos de mayor importancia para la institución en cuanto a seguridad de la información son los siguientes:

- Cuarto de telecomunicaciones
- Servidor de base de datos
- Servidor de correo

5.2.1.1.2. Identificación de amenazas

Una vez identificados los activos se procede a identificar las amenazas que puede afectar a cada activo, considerando que una amenaza puede desencadenar otras.

5.2.1.1.3. Valoración de amenazas

Para la valoración de amenazas se estima la frecuencia y degradación de las que se vio necesario realizar de forma manual para una mejor comprensión. Una vez identificadas las amenazas hay que estimar cuan vulnerable es el equipo activo.

En la Tabla 17, se denota la degradación que mide el daño causado por un incidente en el supuesto caso de que suceda. Caracterizando la fracción del valor activo.

Tabla 17. Indicativo para la degradación.

Niveles	Degradación
0% - 25%	Poco (P)
26% - 50%	Medio (M)
51% - 75%	Alto (A)
76% - 100%	Muy

Obtenido de: (Álvarez, 2014)

Aquellos activos que reciben una calificación de impacto y/o muy alto deben ser objeto de atención inmediata y los que reciban una calificación de riesgo alto, deben ser objeto de planificación inmediata de salvaguardas.

En la Tabla 18, se visualiza la valoración de la frecuencia con la que cada amenaza sucede, se toma en cuenta como una tasa anual de ocurrencia.

Tabla 18. Valorización de la frecuencia.

Periodicidad	Frecuencia
360	A diario
12	Mensualmente
4	Cuatro veces al año
2	Dos veces al año
1	Una vez al año
1/12	Cada varios años

Obtenido de: (Álvarez, 2014)

En la Tabla 19 se indica la frecuencia y degradación de los equipos activos.

Tabla 19. Valorización de amenazas.

	Activos	Amenazas	Frecuencia	Degradación
Instalaciones	Cuarto de telecomunicaciones	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Emanaciones electromagnéticas Manipulación de Programas	2	75%
Personal	Administradores de red	Indisponibilidad del personal Deficiencias en la organización Fugas de información Extorsión Ingeniería social	12	75%
Equipamiento	Servidores	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de	2	25%

		temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Divulgación de información Manipulación de programas		
Datos	Información almacenada en la base de datos	Errores del administrador Alteración accidental de la información Destrucción de información Fuga de información Suplantación de identidad del usuario Abuso de privilegios de acceso Acceso no autorizado Modificación deliberada de la información Destrucción de información Divulgación de información	12	75%

Elaborado por: Los autores.

En la tabla anterior se observa que el activo con mayor porcentaje de degradación y mayor frecuencia de que las amenazas tengan algún impacto sobre el mismo es la información almacenada en la base de datos.

5.2.1.1.4. Identificación de salvaguardas

Después de haber identificado todas las amenazas se procede a identificar los mecanismos de salvaguardas que tienen los activos, describiendo las dimensiones de seguridad que ofrecen entre disponibilidad, integridad, confidencialidad y autenticidad. Dentro del cálculo de riesgos las salvaguardas tienen dos formas de hacerlo:

5.2.1.1.4.1. Reduciendo la frecuencia de amenazas

También conocidas como salvaguardas preventivas, su función ideal sería mitigar completamente la amenaza.

5.2.1.1.4.2. Limitando el daño causado

Existen salvaguardas que de forma directa limitan el posible daño, mientras otras permiten detectar de manera inmediata el ataque para impedir que la degradación continúe.

Algunas salvaguardas solo permiten la pronta recuperación del sistema cuando la amenaza se destruye. Para cualquier versión la amenaza se materializa, pero las consecuencias se detienen, la principal característica de las salvaguardas es su eficacia frente al riesgo.

Como primera salvaguarda ante una amenaza en contra de los datos / información que manejan los usuarios y que contienen los equipos, es el uso de un directorio activo en el dominio de la institución, puesto que actualmente laboran en un "Grupo de trabajo".

En la Tabla 20, se observa las salvaguardas que tienen los activos de red que han sido identificados con sus respectivas dimensiones de seguridad que ofrecen los mismos.

Tabla 20. Salvaguardas para activos de red.

	Activos	Salvaguardas
Instalaciones	Cuarto de telecomunicaciones	Control de acceso físico Aseguramiento de la disponibilidad Alarmas Ventilación
Personal	Administradores de red	Formación y concienciación Aseguramiento de la disponibilidad
Equipamiento	Servidores	Claves
Datos	Información almacenada en la base de datos	Protección de la información

Elaborado por: Los autores

5.2.1.1.5. Estimación del impacto

En el último paso se conocerá el alcance del daño producido, resultado de la materialización de las amenazas sobre los activos.

Tabla 21. Impactos de parámetros.

Parámetro	Concepto	Dimensión	Causas
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requiera a la información y a sus activos asociados	Alto	Podrían darse interrupciones en las actividades de la institución que tendrían un impacto significativo. Administración y gestión: Podría impedir la función efectiva de la institución. Podría causar una publicidad negativa generada por afectar gravemente la relación con el público en general. Obligaciones legales: Podría causar un incumplimiento grave de alguna ley. Información personal: Podría afectar gravemente a un grupo de individuos. Seguridad: Podría causar un incidente grave de seguridad o dificultar una investigación de incidentes graves.
Integridad	Garantía de la exactitud y completitud de la información y los métodos de procesamiento.	Alto	Impida la investigación de delitos graves o facilite su comisión. Administración y gestión: Podría impedir la operación efectiva de la institución. Intereses comerciales o económicos: causa de graves pérdidas económicas. Obligaciones legales: podría causar un incumplimiento grave de una ley o regulación. Información personal: podría afectar gravemente a un grupo de individuos.
Confidencialidad	Es el aseguramiento de	Medio	Podría causar cierta publicidad negativa: para afectar negativamente a las relaciones

	que la información es accesible solo para aquellos autorizados a tener acceso.		con otras instituciones, para afectar negativamente a las relaciones con el público. Información personal: probablemente quebrante leyes o regulaciones.
Autenticidad	Es el aseguramiento de la identidad u origen.	Alto	Administración y gestión: podría impedir la operación efectiva de la institución. Intereses comerciales o económicos: causa de graves pérdidas económicas. Obligaciones legales: podría causar un incumplimiento grave de una ley o regulación. Información personal: podría quebrantar seriamente la ley o algún reglamento de protección de información personal. Seguridad: podría ser la causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

Elaborado por: Los autores

5.2.2. Análisis de vulnerabilidades con software

Para el correcto diagnóstico de la red se realizará el análisis de puertos y vulnerabilidades descrito a continuación:

5.2.2.1. Escaneo de puertos

Para explorar los puertos se consideró utilizar el comando NMAP incluyendo parámetros que no sean fácil de detectar por firewall o detectores de intrusos.

El escaneo de puertos para la red LAN de la institución facilitará la siguiente información:

- Detectar sistemas vivos ejecutando procesos en la red.
- Detectar los puertos que están abiertos o tienen servicios en ejecución.
- Detectar OS fingerprints.

- Detectar direcciones IP en la red o sistemas planteados como objetivos.
- Identificar banners

Las líneas de comandos para el análisis de puertos abiertos para los protocolos TCP/UDP de los servidores de la Gobernación son:

- Nmap -sV -sS -O 192.168.xxx.xxx
- Nmap -sV -sU -O 192.168.xxx.xxx

Los parámetros usados con el comando nmap tienen las siguientes funciones:

- **-sV:** Búsqueda de puertos abiertos para determinar el servicio.
- **-sS:** Escaneo de tipo SYN/Connect
- **-O:** Detecciòn del Sistema operativo
- **-sU:** Escaneo de puertos UDP

A continuación, se visualiza los datos obtenidos a través de las líneas de comando sobre los servidores de la institución:

- **Servidor Asterisk**

```
C:\Users\christian.ayala>nmap -sV -sS -O 192.168.2.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 22:19 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.2.3
Host is up (0.00057s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 4.3 (protocol 2.0)
80/tcp   open  http        nginx 1.1.14
111/tcp  open  rpcbind     2 (RPC #100000)
2000/tcp open  cisco-sccp?
3306/tcp open  mysql       MySQL (unauthorized)
4445/tcp open  upnotifyp?
MAC Address: 00:27:0E:35:87:A4 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
```

Figura 18. NMAP/TCP del servidor Asterisk
Elaborado por: Los autores

```
C:\Users\christian.ayala>nmap -sV -sU -O 192.168.2.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 22:26 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.2.3
Host is up (0.00012s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE   VERSION
111/udp  open          rpcbind   2 (RPC #100000)
123/udp  open          ntp       NTP v4 (secondary server)
5000/udp open|filtered upnp
5060/udp open          sip-proxy FreePBX 2.9.0 (Asterisk 1.8.7.0)
MAC Address: 00:27:0E:35:87:A4 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Device: PBX
```

Figura 19.NMAP/UDP del servidor Asterisk
Elaborado por: Los autores

- **Servidor Zimbra**

```
C:\Users\christian.ayala>nmap -sV -sS -O 192.168.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 22:49 Hora est. PacÝfico, SudamÚrica
Nmap scan report for zimbra.goberguayas.gob.ec (192.168.2.6)
Host is up (0.00055s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Zimbra http config
110/tcp   open  pop3         Zimbra pop3d
111/tcp   open  rpcbind      2-4 (RPC #100000)
143/tcp   open  imap         Zimbra imapd
389/tcp   open  ldap         OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http     Zimbra http config
465/tcp   open  ssl/smtp     Postfix smtpd
514/tcp   open  shell?
587/tcp   open  smtp         Postfix smtpd
993/tcp   open  ssl/imap     Zimbra imapd
995/tcp   open  ssl/pop3     Zimbra pop3d
5222/tcp  open  xmpp-client?
7025/tcp  open  lmtp         Zimbra lmtpd
10000/tcp open  http         MiniServ 1.900 (Webmin httpd)
MAC Address: E4:1F:13:B7:BA:B6 (IBM)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host:  zimbra.goberguayas.gob.ec
```

Figura 20. NMAP/TCP del servido Zimbra
Elaborado por: Los autores

```
C:\Users\christian.ayala>nmap -sV -sU -O 192.168.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 22:55 Hora est. PacÝfico, SudamÚrica
Nmap scan report for zimbra.goberguayas.gob.ec (192.168.2.6)
Host is up (0.000036s latency).
Not shown: 995 closed ports
PORT      STATE         SERVICE VERSION
111/udp   open          rpcbind 2-4 (RPC #100000)
514/udp   open|filtered syslog
1001/udp  open          rpcbind 2-4 (RPC #100000)
5353/udp  open          mdns    DNS-based service discovery
10000/udp open          webmin  (https on TCP port 10000)
MAC Address: E4:1F:13:B7:BA:B6 (IBM)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figura 21. NMAP/UDP del servidor Zimbra.
Elaborado por: Los autores

- **Biométrico**

```
C:\Users\christian.ayala>nmap -sV -sS -O 192.168.2.12
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 22:54 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.2.12
Host is up (0.00043s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE    VERSION
135/tcp  open  tcpwrapped
139/tcp  open  tcpwrapped
445/tcp  open  tcpwrapped
1433/tcp open  tcpwrapped
3389/tcp open  tcpwrapped
7200/tcp open  tcpwrapped
MAC Address: 00:1C:C0:6B:6C:86 (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
```

Figura 22. NMAP/TCP del Biométrico
Elaborado por: Los autores

```
C:\Users\christian.ayala>nmap -sV -sU -O 192.168.2.12
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-20 23:20 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.2.12
Host is up (0.00064s latency).
Not shown: 992 closed ports
PORT     STATE         SERVICE      VERSION
123/udp  open          ntp?
137/udp  open          netbios-ns?
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1025/udp open|filtered blackjack
1434/udp open|filtered ms-sql-m
4500/udp open|filtered nat-t-ike
MAC Address: 00:1C:C0:6B:6C:86 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figura 23. NMAP/UDP del Biométrico
Elaborado por: Los autores

5.2.2.2. Análisis con Nessus

El objetivo principal del análisis de vulnerabilidades es la identificación y documentación de vulnerabilidades del software y equipos host a utilizar. Este tipo de procesos sirve para identificar problemas críticos por los que un intruso podría vulnerar o extraer información confidencial de la institución.

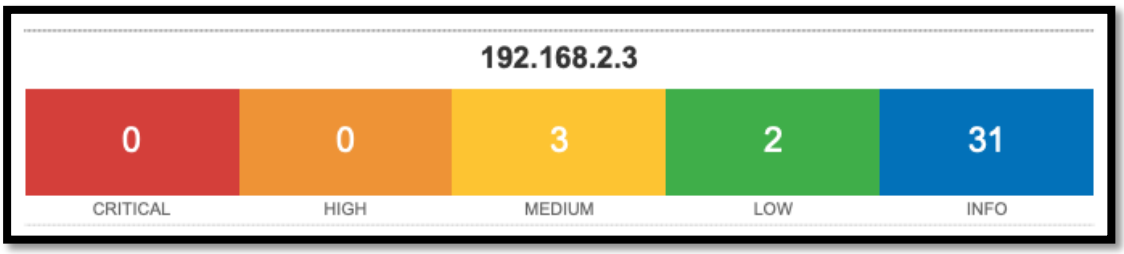
Se procede a realizar el análisis posterior a la exploración de los puertos en los equipos principales de la red, se analizarán las vulnerabilidades asociadas a los servicios de los puertos abiertos para la implementación de una solución óptima de las debilidades. Para lo que es necesario utilizar un software que posea base de datos de vulnerabilidades que han sido identificadas y publicadas en internet, donde entre las más conocidas están, Natural Vulnerabiliy, Security Tech Center y Simantec Connect.

Nessus provee la siguiente información:

- Falta de parches de seguridad
- Configuraciones vulnerables en el sistema
- Exploración de puertos del sistema

A continuación, se presenta el reporte de las vulnerabilidades encontradas mediante el software en los principales equipos de la red:

- **Servidor Asterisk**

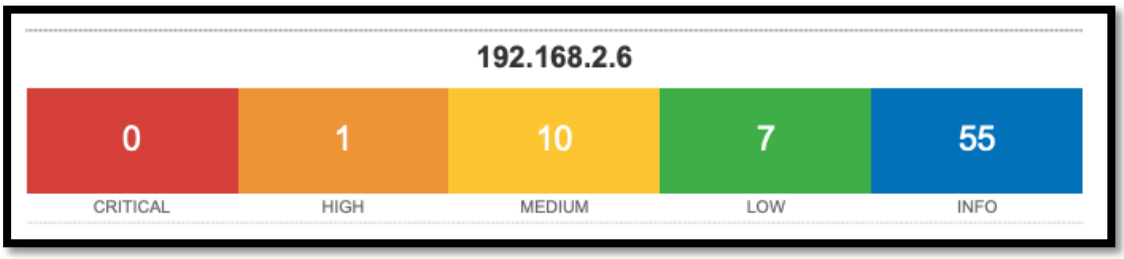


Vulnerabilities Total: 36

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.0	71783	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	63202	Asterisk Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	20834	Inter-Asterisk eXchange Protocol Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

Figura 24. Vulnerabilidades del servidor Asterisk
Elaborado por: Los autores

- **Servidor Zimbra**

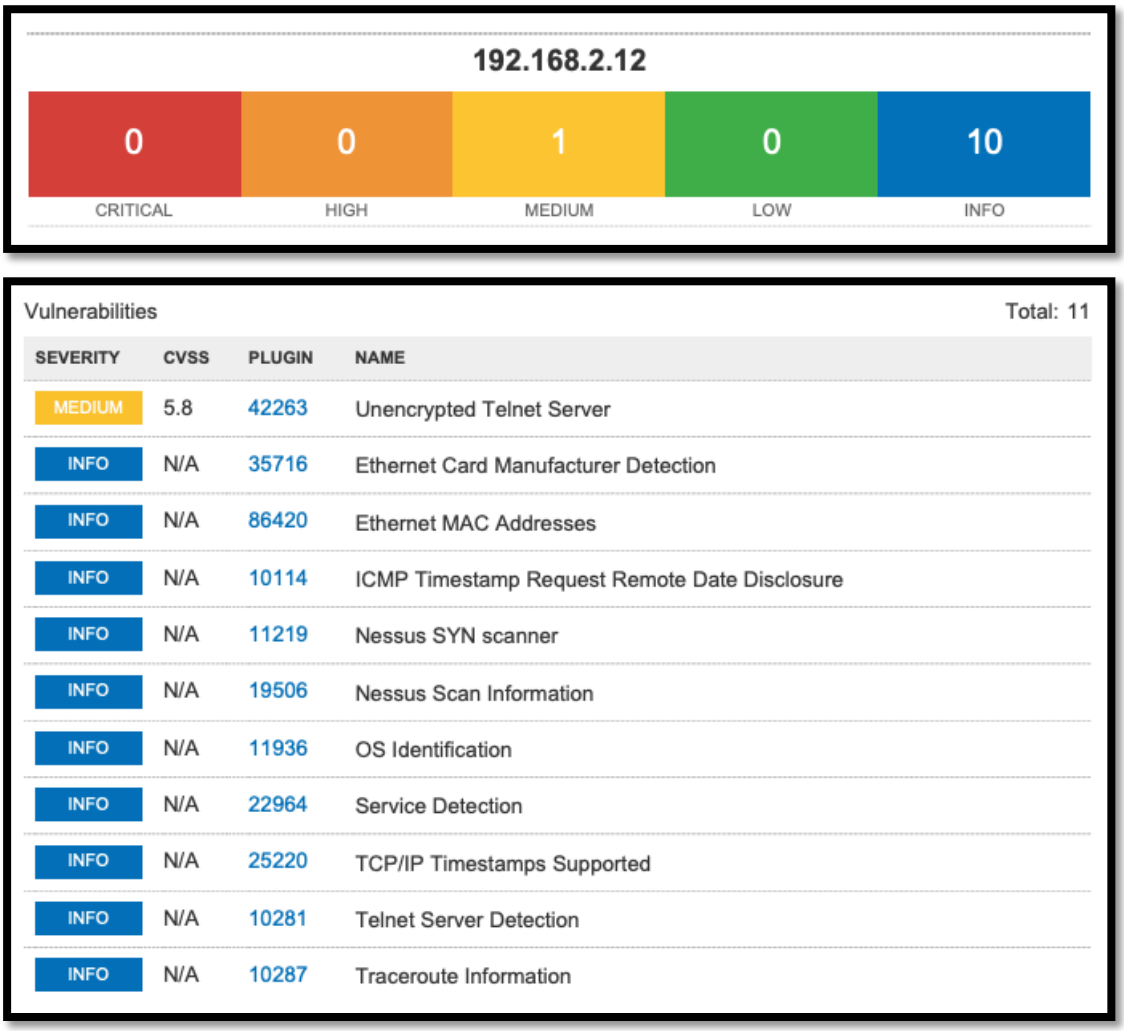


Vulnerabilities — Total: 73

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6	91572	OpenSSL AES-NI Padding Oracle MitM Information Disclosure
LOW	2.6	15855	POP3 Cleartext Logins Permitted
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
INFO	N/A	46180	Additional DNS Hostnames

Figura 25. Vulnerabilidades del servidor zimbra
Elaborado por: Los autores

- **Biométrico**

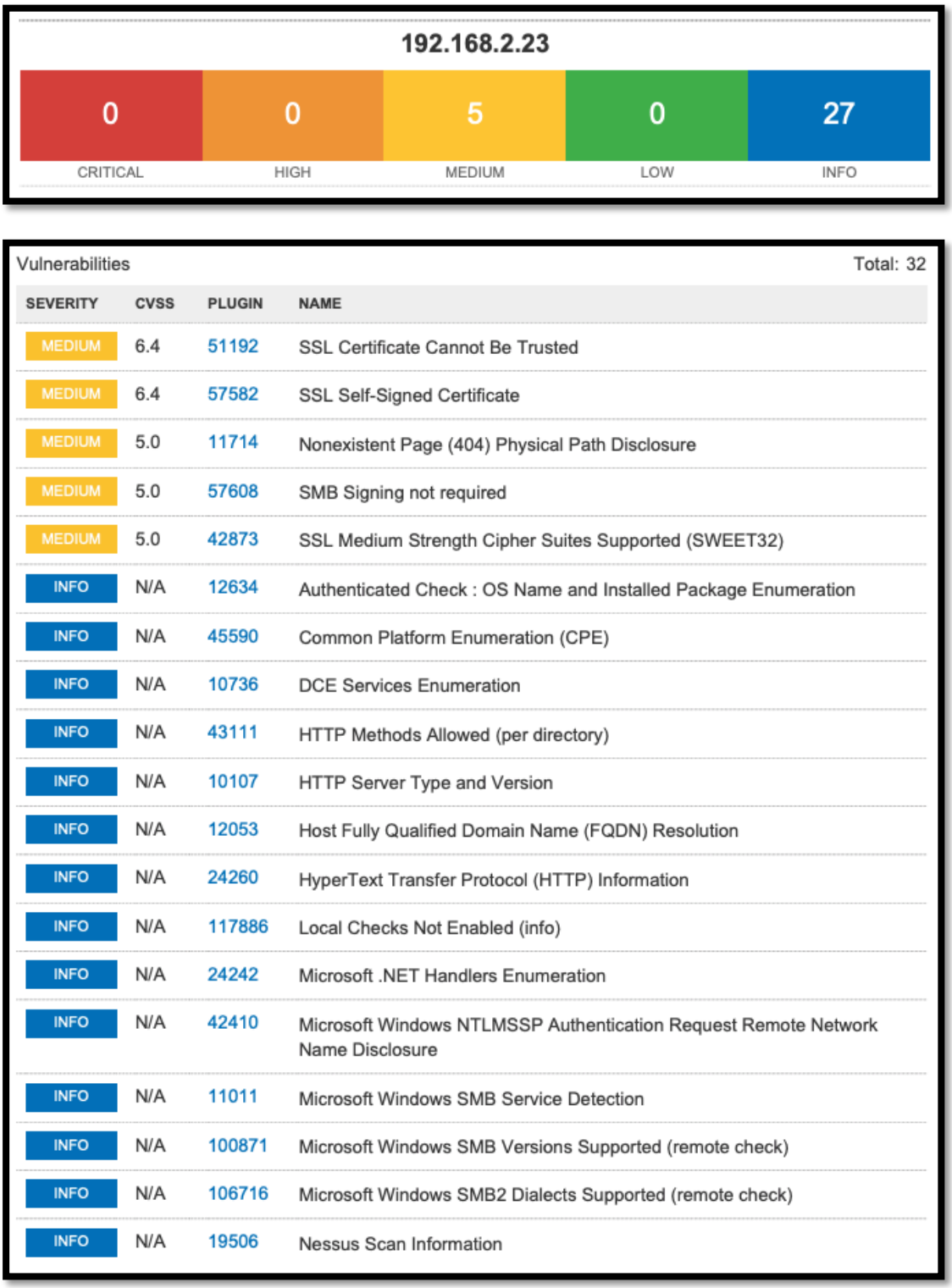


Vulnerabilities — Total: 11

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.8	42263	Unencrypted Telnet Server
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information

Figura 26. Vulnerabilidades del servidor del biométrico
Elaborado por: Los autores

- **Equipo del administrador de red**



192.168.2.23

0	0	5	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 32

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11714	Nonexistent Page (404) Physical Path Disclosure
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	24242	Microsoft .NET Handlers Enumeration
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	19506	Nessus Scan Information

Figura 27. Vulnerabilidades en la PC del administrador de red.
Elaborado por: Los autores

5.2.2.3. Diagnóstico de la Red

Una vez realizado el escaneo de vulnerabilidades a los principales dispositivos, Se reconocen determinadas deficiencias que conllevan a potenciales amenazas para la seguridad; entre las potenciales amenazas que se encontrarán en el sistema están las siguientes:

- Servicios levantados de manera innecesaria.
- No existe una jerarquía, se usa grupo de trabajo.
- Puertos TCP/UDP abiertos.
- Fácil acceso a ciertos archivos privados que contienen información delicada.
- Como única barrera de defensa ante virus, malware y demás formas de infección solo tienen Windows defender.

5.2.3. Análisis del tráfico basado en los servicios internos y externos

Para analizar el tráfico se consideró algunos servicios que brinda la Gobernación del Guayas, como: correo electrónico, base de datos, descarga de archivos y páginas web.

5.2.3.1. Tráfico de correo electrónico

Se consideró que un correo electrónico interno pesa aproximadamente 50Kb y que se revisa un correo por hora, el cálculo sería:

$$AB(correo\ interno) = usuario\ x\ \frac{50Kb}{correo} x \frac{1024\ bits}{1Kb} x \frac{2\ correo}{1\ hora} x \frac{1\ hora}{60\ min} x \frac{1\ min}{60\ s}$$

Ecuación 1 Fórmula para calcular ancho de banda de correo interno
Obtenido de: (Vasco, 2010)

El tráfico para el correo interno será de: $AB(correo\ interno) = 28.44\ bps$

Para un correo electrónico externo se consideró que pesa 200 Kb aproximadamente y que se revisa un correo por hora.

$$AB(correo\ externo) = usuario\ x\ \frac{200Kb}{correo} x \frac{1024\ bits}{1Kb} x \frac{2\ correo}{1\ hora} x \frac{1\ hora}{60\ min} x \frac{1\ min}{60\ s}$$

Ecuación 2 Fórmula para calcular ancho de banda de correo externo
Obtenido de: (Vasco, 2010)

El tráfico para el correo externo será de: $AB\ (correo\ externo) = 137.77\ bps$

5.2.3.2. Tráfico de base de datos

La base de datos que tiene la Gobernación del Guayas es utilizada para almacenar y ordenar la información de sus empleados y la ciudadanía en general. Se estima un promedio de 125 equipos de cómputo en la institución, cada una en su departamento correspondiente, es decir que si todos los usuarios se conectan a la base de datos simultáneamente cada media hora a la base de datos tiene un peso aproximado de 50 Kb, el cálculo sería el siguiente:

$$AB = \frac{50Kb}{usuario} x \frac{1024\ bits}{1Kb} x \frac{1\ hora}{1\ hora} x \frac{1\ hora}{3600\ s}$$

Ecuación 3 Fórmula para calcular ancho de banda del acceso a la base de datos interno
Obtenido de: (Vasco, 2010)

El tráfico para base de datos es: $AB = 14.22\ bps$

5.2.3.3. Tráfico de descarga de archivos

El tamaño promedio de una descarga de internet es de 5mb; para una descarga de 1mb el tiempo aceptable es de 1 minuto. El cálculo es el siguiente:

$$AB = 1\ usuario\ x\ \frac{5120\ kb}{usuario} x \frac{1024\ bits}{1\ kb} x \frac{1}{5\ min} x \frac{1\ min}{60\ s}$$

Ecuación 4 Fórmula para calcular ancho de banda de una descarga promedio
Obtenido de: (Vasco, 2010)

El tráfico de una descarga promedio será: $AB = 87381.33\ bps$

5.2.3.4. Tráfico de páginas web

Los usuarios utilizan el servicio de internet sin ninguna restricción, se estimó que cada uno accede a un promedio de 10 páginas por hora y cada una pesa 3mb aproximadamente.

$$AB = 1\ usuario\ x\ \frac{3072\ kb}{usuario} x \frac{1024\ bits}{1\ kb} x \frac{10\ páginas}{1\ hora} x \frac{1\ hora}{3600\ s}$$

Ecuación 5 Fórmula para calcular ancho de banda del acceso a una página web
Obtenido de: (Vasco, 2010)

El tráfico aproximado para páginas webs es: $AB = 8738.133\ bps$

En la tabla 22, se detallan los resultados obtenidos a partir de los cálculos realizados anteriormente para el tráfico interno por usuario en kbps.

Tabla 22. Demanda de tráfico actual.

Servicios Internos	Capacidad Individual (kbps)
Correo Interno	0.0284
Correo Externo	0.1377
Base de Datos	0.014
Descargas	84.381
Páginas web	8.738
Total	**93.291**

Elaborado por: Los autores

Por los cálculos realizados se determinó que cada usuario necesita 93.291 Kbps y para que los 100 usuarios conectados al mismo tiempo es necesario una capacidad de al menos 10 Mbps.

La Gobernación posee contratado un Plan CNT con capacidad de 20 Mbps, el mismo que se distribuye para uso de los usuarios y equipos de la institución.

5.2.4. Análisis para la selección e implementación de un mecanismo de seguridad perimetral

Para poder seleccionar de manera adecuada el UTM Appliance que va a brindar seguridad a la Gobernación debemos realizar una comparación de los puntos más importantes entre algunas soluciones UTM.

La comparación será realizada entre productos que son adecuados para organizaciones que poseen entre 50 y 100 usuarios donde se medirán 4 funciones que serían las más importantes al momento de adquirir la solución UTM:

- **Rendimiento de firewall**: Esta es la función primordial en un UTM. Cualquier inconveniente de aquí afecta a todo el tráfico que pasa por el dispositivo. Por lo que el rendimiento de firewall idealmente debería permitir la tasa de línea para sus conexiones. La prueba se realizó con tres puertos de 1Gbps, dando como máximo teórico de 3Gbps.
- **Rendimiento de control de aplicación**: Permite monitorear y administrar de manera efectiva los diferentes tipos de tráfico. Pasando por su puerta de enlace como VPN, Youtube o Facebook sin tener que bloquear el tráfico por completo. Esta prueba analiza el rendimiento de la Capa 7. Para analizar el

tráfico en esta capa se necesita ensamblar varios paquetes de tráfico para poder determinar la aplicación usada.

- **Rendimiento IPS**: Los sistemas de prevención contra intrusos monitorean la red en busca de tráfico sospechoso y pueden bloquear las vulnerabilidades conocidas. Al igual que el control de aplicaciones, este es un proceso de uso intensivo de recursos donde los paquetes son ensamblados e inspeccionados.
- **Conexiones por segundo**: En esta prueba se verifica el número máximo de nuevas conexiones TCP que un dispositivo de seguridad puede establecer por segundo. El establecimiento de conexiones TCP consume muchos recursos y usualmente sortea recursos del motor de detección de seguridad del dispositivo. El número máximo de nuevas conexiones establecidas por segundo da una indicación de la capacidad de los dispositivos para mantener la seguridad sin afectar su rendimiento.

Tabla 23. Comparación entre dispositivos de seguridad perimetral.

	Sohpos SG 210	**Dell SonicWall NSA 2600**	**Fortinet Fortigate 100 D**	**WatchGuard XTM 525**
Rendimiento del Firewall	3000 Mbps	1884 Mbps	1322 Mbps	1886 Mbps
Rendimiento de control de la aplicación	1090 Mbps	486 Mbps	679 Mbps	461 Mbps
Rendimiento IPS	504 Mbps	132 Mbps	420 Mbps	475 Mbps
Conexiones por segundo	29660	8800	3200	15100

Elaborado por: Los autores

Del cuadro comparativo se define que: En las pruebas independientes basadas en escenarios de la vida real, el dispositivo de Sophos entregó el mejor rendimiento, incluso cuando se habilitan funciones adicionales de seguridad y control, superando a las soluciones comparativas de las otras marcas.

5.2.5. Análisis del direccionamiento de la red

De acuerdo con la información obtenida y a la necesidad de maximizar la eficiencia del direccionamiento de la red, se propone el uso de VLSM.

Ya que la red no se considera de tamaño “grande” puesto que los hosts no superan a los 100 aproximadamente, y debido a que la institución cuenta en ciertos departamentos con un usuario, no es recomendable implementar el subneteo de la red principal en subredes del mismo tamaño, puesto que esto significaría un desperdicio y mala planificación del direccionamiento de la red.

Por su parte, VLSM, permite que la organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red, brindando de esta forma una mayor flexibilidad a las subredes que se generarán de acuerdo con el número de usuarios en cada departamento.

5.2.6. Análisis de la Norma ANSI/TIA/EIA 606A

Teniendo en consideración que ningún sistema de cableado puede ser administrado correctamente sin un etiquetado lógico y claro; y, frente a uno de los inconvenientes principales que dificulta la ejecución de una de las funciones del departamento de Tecnología por el tiempo de respuesta ante el requerimiento de habilitación o verificación del estado de un punto de red y de acuerdo a la necesidad de la institución, se recomienda la aplicación del Estándar de administración para la infraestructura de telecomunicaciones en edificios comerciales TIA/EIA 606, norma de especificación sobre el rotulado de los cables TIA/EIA 606A.

5.3. Diseño

5.3.1. Diseño del esquema de seguridad

Para diseñar un correcto esquema de seguridad para la red se tomaron en cuenta todos los puntos tratados anteriormente, desde el levantamiento de información hasta los análisis realizados tanto de manera teórica como práctica para la correcta implementación de equipos y software, como primera instancia se implementó un Servidor de dominio Active Directory en un equipo que fue provisto por la Unidad de Tecnología, y un Firewall UTM de la marca Sophos, modelo SG 210, la adquisición del mismo fue realizada por la institución a la empresa “Innovative”.

Las especificaciones técnicas de ambos equipos se detallarán a continuación:

- **Especificaciones técnicas del servidor de dominio**

Figura 28. Servidor de dominio.
Obtenido de: https://bit.ly/2K5000x

- **Marca:** IBM
- **Modelo:** X3650 M3
- **Procesador:** 1 CPU Xeon 2,4Ghz
- **RAM:** 8Gb
- **Disco Duro:** 300Gb x 4
- **Raid:** Raid 0
- **Sistema operativo:** Windows Server 2008 R2 Standard

- **Especificaciones técnicas del firewall UTM**

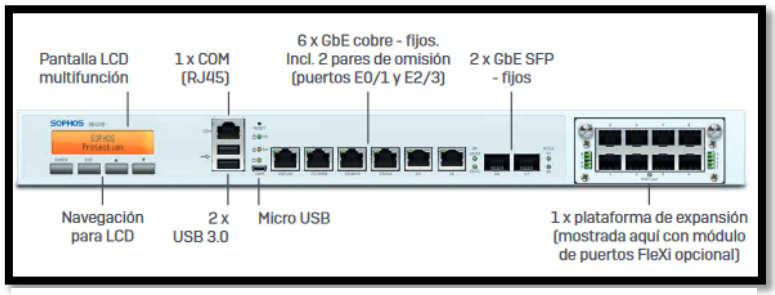


Figura 29 Especificaciones técnicas del firewall UTM
Obtenido de: https://www.sophos.com

- **Marca:** Sophos
- **Modelo:** SG 210
- **Procesador:** Intel Celeron CPU G1820 2.7 Ghz
- **RAM:** 8Gb
- **Disco duro:** SSD 120 Gb
- **Sistema Operativo:** Sophos UTM 9 Versión 9.506-2

A continuación, se describe gráficamente el diseño del esquema de red con seguridad perimetral.

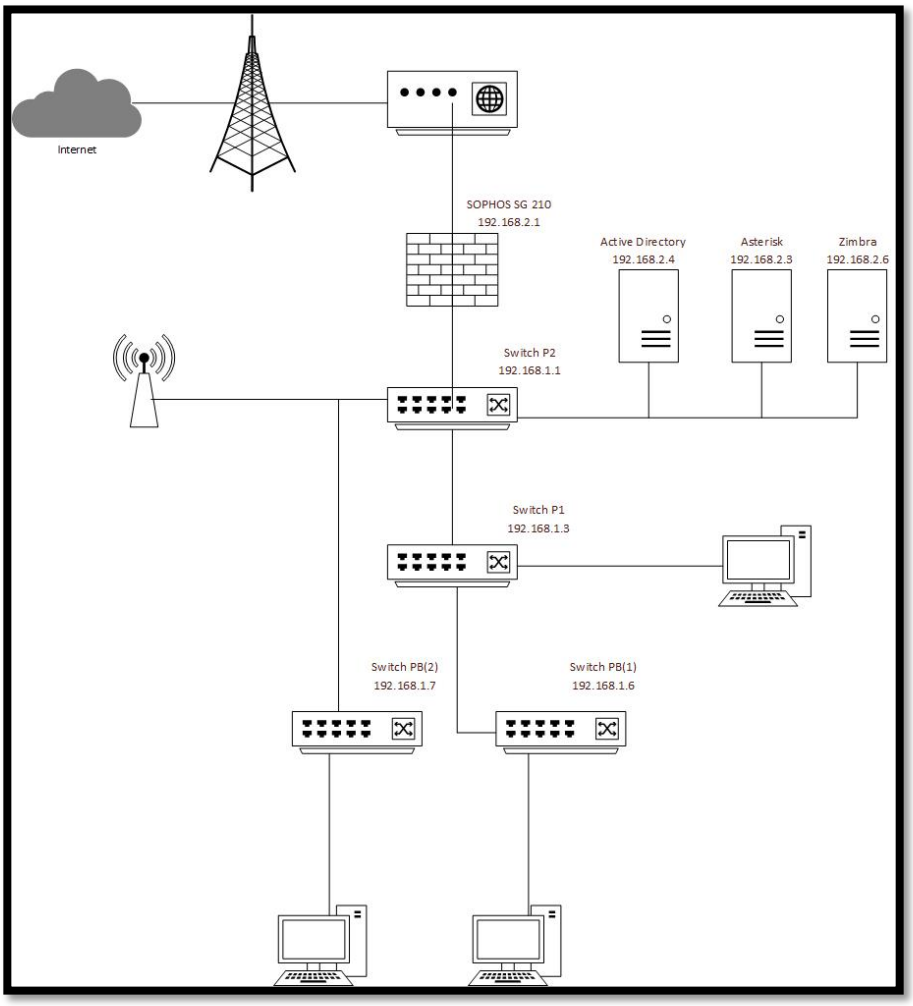


Figura 30. Esquema de seguridad para la Gobernación del Guayas
Elaborado por: Los autores

5.3.2. Planificación del direccionamiento IP – VLAN y VLSM

Para optimizar las direcciones IPs actuales y generar un correcto diseño de subredes, se tabulará la información actual:

Tabla 24. Configuración actual de la red.

ACTUALIDAD	NOMBRE VLAN	Rango IP
Switches y Access point, Firewall	CONECTIVIDAD	192.168.1.0/24
Servidores, impresoras, usuarios	SERVERS	192.168.2.0/24
Telefonía IP	TELEFONICA	192.168.3.0/24

Elaborado por: Los autores.

Se identificó la cantidad de usuarios por piso, para agruparlos y definir las VLAN necesarias para definir el crecimiento estimado. Este análisis se basa en un crecimiento del 100% en los próximos 5 años.

- **Planta Baja**

Tabla 25. Detalle de usuarios de Planta Baja.

Departamento	Número de usuarios	Tipo de usuario	Usuarios totales	Crecimiento estimado
Choferes - Contraloría	4	Interno	24	48
Financiero	8	Interno		
Secretaria	5	Interno		
Recepción	1	Interno		
Administrativo	6	Interno		
Ministerio del interior	9	Externo	9	18

Elaborado por: Los autores.

- **Primer piso**

Tabla 26. Detalle de usuarios de Primer Piso.

Departamento	Número de usuarios	Tipo de usuario	Usuarios totales	Crecimiento estimado
Talento Humano	8	Interno	28	56
Jurídico	7	Interno		
Comunicación	10	Interno		
Salas de reunión	3	Interno		
Jefatura Política	9	Externo	12	24
Frente Social	3	Externo		

Elaborado por: Los autores.

- **Segundo piso**

Tabla 27. Detalle de usuarios de Segundo Piso.

Departamento	Número de usuarios	Tipo de usuario	Usuarios totales	Crecimiento estimado
TIC	4	Interno	4	8
Planificación	6	Interno	15	30
Seguridad Ciudadana	5	Interno		
Intendencia	2	Interno		
Sub intendencia	2	Interno		
Gobernador	7	VIP	7	14

Elaborado por: Los autores.

Se puede observar en las tablas que ciertas áreas contienen cantidades pequeñas de usuarios, por lo que se sugiere realizar un agrupamiento por cada piso de tal forma que al subdividir las redes se garantice una optimización en el uso de los segmentos de red, y que se independice dichos grupos controlando su acceso por piso.

Adicional se considera grupos de usuarios internos, externos y VIP. Esta diferenciación se la realiza para de manera práctica impulsar conceptos de separación de accesos, donde cada grupo de usuarios tendrán de manera distinta accesos a los diferentes segmentos de red y navegación a internet.

Los usuarios externos simulan una red de terceros, los mismos que deben ser controlados al momento de acceder a servicios de la red productiva. Los usuarios VIP representan un grupo de usuarios con privilegios diferencias y que tiene acceso a sitios que normalmente no se brindan a los usuarios internos de la institución.

De esta forma se sugiere el siguiente agrupamiento:

Tabla 28. Detalle de agrupamiento para VLAN.

DEPARTAMENTO	NOMBRE VLAN	ID VLAN
CHOFERES CONTRALORÍA	VLAN PB	VLAN 5
FINANCIERO		
SECRETARIA		
RECEPCIÓN		
ADMINISTRATIVO		
TALENTO HUMANO	VLAN PISO 1	VLAN 4
JURÍDICO		
COMUNICACIÓN		
SALAS DE REUNIÓN		
PLANIFICACIÓN	VLAN PISO 2	VLAN 7
SEGURIDAD CIUDADANA		
INTENDENCIA		
SUB INTENDENCIA		
ADMINISTRATIVO		
MINISTERIO DEL INTERIOR	VLAN TERCEROS	VLAN 6
JEFATURA POLITICA		
FRENTE SOCIAL		
GOBERNADOR	VLAN VIP	VLAN 8

Elaborado por: Los autores.

Es importante mencionar que las impresoras pertenecerán al segmento IP de cada piso donde estén ubicadas.

A continuación, se procede a aplicar VLSM para realizar la subdivisión de los segmentos de red, se reutiliza los segmentos que actualmente ya están implementados y se creará nuevos segmentos de red de acuerdo con las necesidades del diseño.

Tabla 29. Diseño VLSM y VLAN.

NOMBRE DE VLAN	VLAN ID	Usuarios necesarios	Últimos Bits IP									Máximo número de usuarios
			24	25	26	27	28	29	30	31	32	
			2^n									
			8	7	6	5	4	3	2	1	0	
			256	128	64	32	16	8	4	2	1	
ADMIN	99		X									254
SERVERS	2		X									254
TELEFONIA	3		X									254
VLAN P1	4	56			X							62
VLAN PB	5	48			X							62
TERCEROS	6	42			X							62
VLAN P2	7	30				X						30
VLAN VIP	8	14					X					16

Elaborado por: Los autores.

Tabla 30. Segmentos asignados por VLAN.

Segmento de red IP asignada			
VLAN	inicio	Fin	RED LAN ID
ADMIN	192.168.1.0	192.168.1.255	192.168.1.0/24
SERVERS	192.168.2.0	192.168.2.255	192.168.2.0/24
TELEFONIA	192.168.3.0	192.168.3.255	192.168.3.0/24
VLAN P1	192.168.4.0	192.168.4.63	192.168.4.0/26
VLAN PB	192.168.4.64	192.168.4.127	192.168.4.64/26
TERCEROS	192.168.4.128	192.168.4.191	192.168.4.128/26
VLAN P2	192.168.4.192	192.168.4.223	192.168.4.192/27
VLAN VIP	192.168.4.224	192.168.4.239	192.168.5.0/28

Elaborado por: Los autores.

De acuerdo con el diseño anteriormente especificado, se procederá a configurar las VLAN en los equipos switches en modo de consola. Para el correcto control e identificación de los switches de cada piso, los mismos serán identificados de la siguiente forma:

Tabla 31. Identificación de Switches por piso.

Piso	Switch	Identificación
Piso 2	SW 3C Core	GOB_SW_CORE
	SW CS Poe	GOB_SW_CS_P2_A1
	SW 2	GOB_SW_3C_P2_A2
	SW 3	GOB_SW_3C_P2_A3
Piso 1	SW 1	GOB_SW_3C_P1_A1
	SW 2	GOB_SW_3C_P1_A2

PB	SW 1	GOB_SW_3C_PB_A1
	SW 2	GOB_SW_3C_PB_A2

Elaborado por: Los autores.

Teniendo finalmente la siguiente configuración en cada Switch:

Tabla 32. Configuración de VLAN en Switches.

Local	Puerto	Modo	Remoto	Puerto remoto
GOB_SW_CORE	Eth 30	TRUNK	GOB_SW_CS_P2_A1	Eth 24
GOB_SW_CORE	Eth 31	ACCESO	Servidor de Mesa de Ayuda	
GOB_SW_CORE	Eth 32	ACCESO	Servidor de Archivos	
GOB_SW_CORE	Eth 33	ACCESO	LAN Sophos	Eth E0
GOB_SW_CORE	Eth 34	TRUNK	GOB_SW_3C_P2_A3	Eth 22
GOB_SW_CORE	Eth 35	ACCESO	Servidor Zimbra	
GOB_SW_CORE	Eth 36	ACCESO	Servidor Zimbra	
GOB_SW_CORE	Eth 37	ACCESO	Cisco CNT	
GOB_SW_CORE	Eth 38	ACCESO	Servidor ASTERISK	
GOB_SW_CORE	Eth 39	ACCESO	Troncal Internet	
GOB_SW_CORE	Eth 47	ACCESO	Sophos	Eth E2
GOB_SW_3C_P2_A2	Eth 21	TRUNK	GOB_SW_3C_P1_A1	Eth 44
GOB_SW_3C_P2_A2	Eth 24	TRUNK	GOB_SW_3C_P2_A3	Eth 24
GOB_SW_3C_P2_A2	Gig 26	TRUNK	GOB_SW_3C_PB_A1	Gig 49
GOB_SW_3C_P2_A3	Eth 18	ACCESO	Servidor de Directorio Activo	
GOB_SW_3C_P1_A1	Eth 45	TRUNK	GOB_SW_3C_PB_A2	Eth 16
GOB_SW_3C_P1_A1	Eth 46	TRUNK	GOB_SW_3C_P1_A2	Eth 24

Elaborado por: Los autores.

5.3.3. Diseñar reglas de seguridad a implementar

5.3.3.1. Políticas por implementar en Sophos

Dentro de las bondades que posee Sophos se debe definir políticas de seguridad en algunos módulos, a continuación, se detallaran de manera resumida ya que en el **Anexo B** se explica de manera detallada.

- **Web Protection,** este módulo controlará la navegación por internet, se configura por defecto la política de bloquear todo lo que no se encuentre en ningún perfil de navegación, para lo que se han creado 2 perfiles:
  - Bloqueo autoridades
  - Bloqueo default
- **Control de aplicaciones**, este módulo filtra a nivel de capa 7 en la navegación por internet. Si bien Web protection controla la navegación,

no bloquea aplicaciones específicas que no operan en navegadores, para lo que se crea 1 política de filtración de aplicaciones:

    - Esta política aplica a todos los funcionarios de la Gobernación, posee los siguientes bloqueos: juegos, proxy, Windows update y Streaming Media.

- **Email protection**, es la primera barrera de verificación antes de ser entregado:
    - Listas RBL, primer filtro contra spam.
- **Reglas de firewall**, principal filtro de la red que realiza algunas acciones como:
    - Bloquea clientes con mala reputación
    - Omite búsquedas remotas para clientes con mala reputación
    - Filtro de amenazas comunes
    - Bloqueo de amenazas comunes
- **Listas negras remitentes**, se configuró 273 direcciones aproximadamente para ser bloqueadas.
- **Filtro de extensiones de archivos**, se configura para restringir ciertos tipos de archivos adjuntos en correo electrónico.
- **WebServer Protection**, protege el acceso web a los servidores. En lugar de crear un NAT en los puertos 80 o 443, se usa este módulo que funciona como proxy inverso para devolver los datos y controlar ataques como: Protocol violations, protocol anomalies, request limits, entre otros.

5.3.3.2. Políticas por implementar en Active Directory

Contando con el dominio “GOBERGUAYAS”, se estableció un listado de las políticas nativas a implementarse dentro de las unidades organizativas “Equipos” y “Usuarios”, las mismas que entre las principales son:

- Configuración de seguridad:
    - Mantener historial de contraseñas.
    - Contraseñas deben cumplir con requisitos de complejidad.
- Componentes de Windows:

- Deshabilitar directivas de personalización de ventanas del escritorio.
- Desactivar directivas para copias de seguridad del equipo cliente.
- Desactivar gadgets de escritorio.
- No permitir la ejecución de Windows Messenger
- Desactivar aplicación de Windows Mail.

- Escritorio:
  - Habilitar el tapiz de escritorio con logo de la institución
- Menú de Inicio y barra de tareas:
  - Bloquear las configuraciones en la barra de tarea
  - Quitar íconos de entretenimiento del menú inicio
- Panel de Control:
  - Permitir agregar o quitar programas (usuarios administradores)
  - Buscar impresoras de toda la red
  - Impedir personalización
- Sistema:
  - Solicitar contraseña al reanudar tras hibernación o suspensión.

5.3.4. Definición de nomenclatura para etiquetado

Acorde a la recomendación de la norma, la identificación de los puntos de red se representará de la siguiente forma:

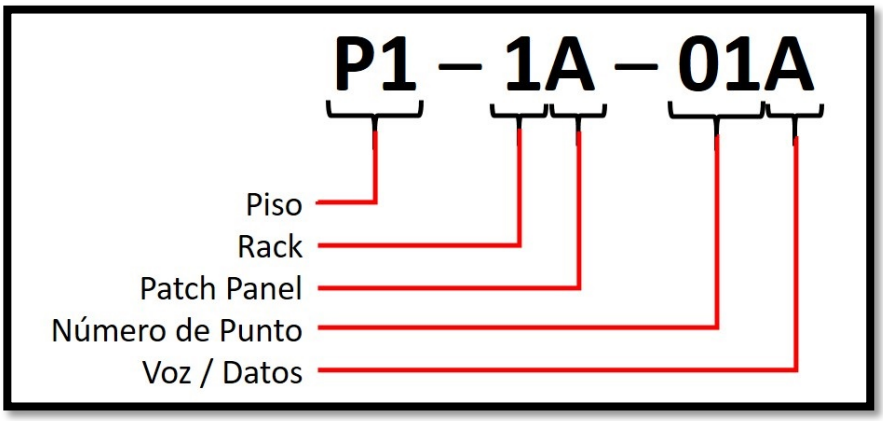


Figura 31. Nomenclatura de identificación de puntos de red
Elaborado por: Los autores.

La numeración se debe realizar en sentido horario, con lo establecido anteriormente, la identificación de los puntos de red sería: P1-1A-01A, la etiqueta

indica que, el punto de red de “voz” se encuentra ubicado en el puerto 01 del Patch panel “A” en el Rack “1” del primer piso.

Los Patch panel de cada gabinete serán identificados con letras, pudiéndose repetir las letras en los diferentes pisos.

Ya que la cantidad de puntos por piso no supera la centena, será representado con número de 2 cifras.

Tal como se especificó en la etapa de levantamiento de la información, la Gobernación de la Provincia del Guayas, en sus comienzos clasificó los puntos como voz y datos, puesto que contaban con una Central de Telefonía Analógica; y; en la actualidad, cuentan con Telefonía IP, motivo por el cual, bajo solicitud explícita de la Unidad de Tecnología y con el fin de mantener un orden coherente en la identificación de los puntos de datos, se identificarán los puntos de datos con la letra “B” y lo puntos de voz con la “A”.

5.4. Implementación

Se procede con la implementación del nuevo esquema de red que integra la configuración en los switches, instalación de Sophos y de Active Directory, y la aplicación de la norma ANSI/TIA/EIA 606, todo esto se efectuó acorde a las políticas que fueron establecidas en conjunto con el personal de la Unidad de Tecnología de la institución. Todo lo anteriormente mencionado se detallará a continuación:

5.4.1. Configuración de VLAN en Switches

Se configuró el Switch Core del Piso 2 de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_CORE
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/30 se estableció como puerto trunk hacía el Switch 1 del Piso 2, permitiendo el paso de las VLAN correspondientes.
- El puerto 1/0/31 se configura en modo acceso a la VLAN 2 ya que éste conecta al Servidor de Mesa de Ayuda.
- El puerto 1/0/32 se configura en modo acceso a la VLAN 2 ya que éste conecta al Servidor de Archivos.

- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

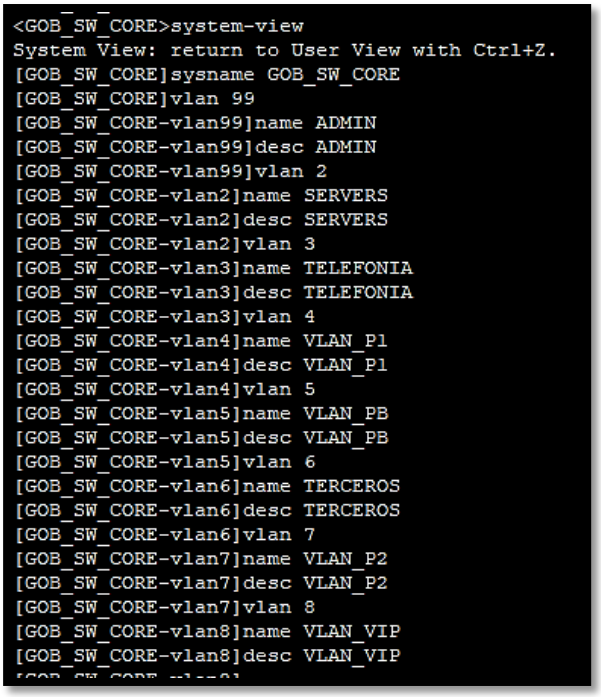


Figura 32 Configuración de VLAN en Switch Core
Elaborado por: Los autores

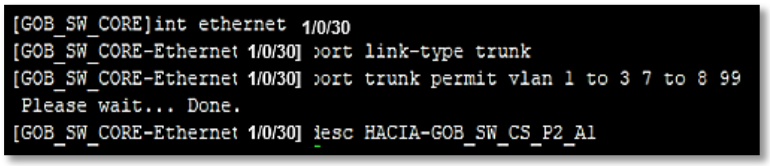


Figura 33 Configuración de puerto modo Trunk en Switch Core
Elaborado por: Los autores

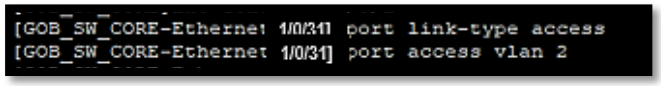


Figura 34. Configuración de puerto modo Acceso en Switch Core
Elaborado por: Los autores

El Switch 2 del Piso 2 se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_P2_A2
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.

- El puerto 1/0/21 se estableció como puerto trunk hacía el Switch 1 del Piso 1, permitiendo el paso de las VLAN correspondientes.
- El puerto 1/0/24 se estableció como puerto trunk hacía el Switch 3 del Piso 2, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
[GOB_SW_CORE]sysname GOB_SW_3C_P2_A2
[GOB_SW_3C_P2_A2]vlan 99
[GOB_SW_3C_P2_A2-vlan99]name ADMIN
[GOB_SW_3C_P2_A2-vlan99]desc ADMIN
[GOB_SW_3C_P2_A2-vlan99]vlan 2
[GOB_SW_3C_P2_A2-vlan2]name SERVERS
[GOB_SW_3C_P2_A2-vlan2]desc SERVERS
[GOB_SW_3C_P2_A2-vlan2]vlan 3
[GOB_SW_3C_P2_A2-vlan3]name TELEFONIA
[GOB_SW_3C_P2_A2-vlan3]desc TELEFONIA
[GOB_SW_3C_P2_A2-vlan3]vlan 4
[GOB_SW_3C_P2_A2-vlan4]name VLAN_P1
[GOB_SW_3C_P2_A2-vlan4]desc VLAN_P1
[GOB_SW_3C_P2_A2-vlan4]vlan 5
[GOB_SW_3C_P2_A2-vlan5]name VLAN_PB
[GOB_SW_3C_P2_A2-vlan5]desc VLAN_PB
[GOB_SW_3C_P2_A2-vlan5]vlan 6
[GOB_SW_3C_P2_A2-vlan6]name TERCEROS
[GOB_SW_3C_P2_A2-vlan6]desc TERCEROS
[GOB_SW_3C_P2_A2-vlan6]vlan 7
[GOB_SW_3C_P2_A2-vlan7]name VLAN_P2
[GOB_SW_3C_P2_A2-vlan7]desc VLAN_P2
[GOB_SW_3C_P2_A2-vlan7]vlan 8
[GOB_SW_3C_P2_A2-vlan8]name VLAN_VIP
[GOB_SW_3C_P2_A2-vlan8]desc VLAN_VIP
[GOB_SW_3C_P2_A2-vlan8]
```

Figura 35 Configuración de VLAN en Switch 2 P2
Elaborado por: Los autores

```
[GOB_SW_3C_P2_A2-vlan8]int ethernet 1/0/21
[GOB_SW_3C_P2_A2-Ethernet1/0/21]port link-type trunk
[GOB_SW_3C_P2_A2-Ethernet1/0/21]port trunk permit vlan 1 to 4 6 8 99
 Please wait... Done.
[GOB_SW_3C_P2_A2-Ethernet1/0/21]desc HACIA_GOB_SW_3C_P1_A1
[GOB_SW_3C_P2_A2-Ethernet1/0/21]
[GOB_SW_3C_P2_A2-Ethernet1/0/21]int  ethernet 1/0/24
[GOB_SW_3C_P2_A2-Ethernet1/0/24]port link-type trunk
[GOB_SW_3C_P2_A2-Ethernet1/0/24]port trunk permit vlan all
 Please wait..................................... Done.
[GOB_SW_3C_P2_A2-Ethernet1/0/24]desc HACIA_GOB_SW_3C_P2_A3
```

Figura 36 Configuración de puertos modo Trunk en Switch 2 P2
Elaborado por: Los autores

```
[GOB_SW_3C_P2_A2-Ethernet1/0/24]int ethernet 1/0/1
[GOB_SW_3C_P2_A2-Ethernet1/0/1]port link-type access
[GOB_SW_3C_P2_A2-Ethernet1/0/1]port access vlan 7
[GOB_SW_3C_P2_A2-Ethernet1/0/1]
[GOB_SW_3C_P2_A2-Ethernet1/0/1]int ethernet 1/0/2
[GOB_SW_3C_P2_A2-Ethernet1/0/2]port link-type access
[GOB_SW_3C_P2_A2-Ethernet1/0/2]port access vlan 7
```

Figura 37 Configuración de puertos modo Acceso en Switch 2 P2
Elaborado por: Los autores

El Switch 3 del Piso 2 se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_P2_A3
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/22 se estableció como puerto trunk hacía el Switch Core del Piso 2, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
[switch]sysname GOB_SW_3C_P2_A3
[GOB_SW_3C_P2_A3]vlan 99
[GOB_SW_3C_P2_A3-vlan99]name ADMIN
[GOB_SW_3C_P2_A3-vlan99]desc ADMIN
[GOB_SW_3C_P2_A3-vlan99]vlan 2
[GOB_SW_3C_P2_A3-vlan2]name SERVERS
[GOB_SW_3C_P2_A3-vlan2]desc SERVERS
[GOB_SW_3C_P2_A3-vlan2]vlan 3
[GOB_SW_3C_P2_A3-vlan3]name TELEFONIA
[GOB_SW_3C_P2_A3-vlan3]desc TELEFONIA
[GOB_SW_3C_P2_A3-vlan3]vlan 4
[GOB_SW_3C_P2_A3-vlan4]name VLAN_P1
[GOB_SW_3C_P2_A3-vlan4]desc VLAN_P1
[GOB_SW_3C_P2_A3-vlan4]vlan 5
[GOB_SW_3C_P2_A3-vlan5]name VLAN_PB
[GOB_SW_3C_P2_A3-vlan5]desc VLAN_PB
[GOB_SW_3C_P2_A3-vlan5]vlan 6
[GOB_SW_3C_P2_A3-vlan6]name TERCEROS
[GOB_SW_3C_P2_A3-vlan6]desc TERCEROS
[GOB_SW_3C_P2_A3-vlan6]vlan 7
[GOB_SW_3C_P2_A3-vlan7]name VLAN_P2
[GOB_SW_3C_P2_A3-vlan7]desc VLAN_P2
[GOB_SW_3C_P2_A3-vlan7]vlan 8
[GOB_SW_3C_P2_A3-vlan8]name VLAN_VIP
[GOB_SW_3C_P2_A3-vlan8]desc VLAN_VIP
[GOB_SW_3C_P2_A3-vlan8]
[GOB_SW_3C_P2_A3-vlan8]
```

Figura 38 Configuración de VLAN en Switch 3 P2
Elaborado por: Los autores

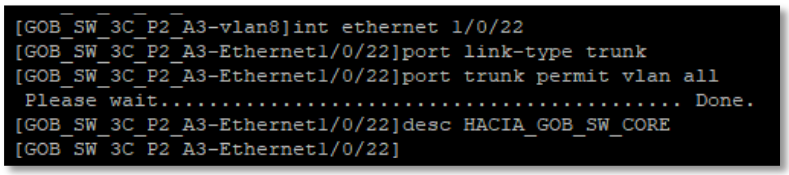


Figura 39 Configuración de puertos modo Trunk en Switch 3 P2
Elaborado por: Los autores

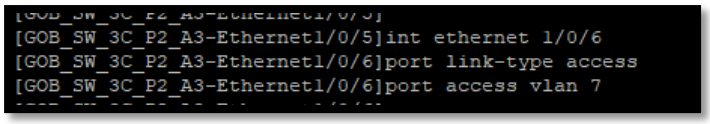


Figura 40 Configuración de puertos modo Acceso en Switch 3 P2
Elaborado por: Los autores

El Switch 1 del Piso 1 se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_P1_A1
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/44 se estableció como puerto trunk hacía el Switch 2 del Piso 2, permitiendo el paso de las VLAN correspondientes.
- El puerto 1/0/45 se estableció como puerto trunk hacía el Switch 2 de Planta Baja, permitiendo el paso de las VLAN correspondientes.
- El puerto 1/0/46 se estableció como puerto trunk hacía el Switch 2 del Piso 1, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
<Gobernacion2>system-view
System View: return to User View with C
[Gobernacion2]
[Gobernacion2]sysname GOB_SW_3C_P1_A1
[GOB_SW_3C_P1_A1]vlan 99
[GOB_SW_3C_P1_A1-vlan99]name ADMIN
[GOB_SW_3C_P1_A1-vlan99]desc ADMIN
[GOB_SW_3C_P1_A1-vlan99]vlan 2
[GOB_SW_3C_P1_A1-vlan2]name SERVERS
[GOB_SW_3C_P1_A1-vlan2]desc SERVERS
[GOB_SW_3C_P1_A1-vlan2]vlan 3
[GOB_SW_3C_P1_A1-vlan3]name TELEFONIA
[GOB_SW_3C_P1_A1-vlan3]desc TELEFONIA
[GOB_SW_3C_P1_A1-vlan3]vlan 4
[GOB_SW_3C_P1_A1-vlan4]name VLAN_P1
[GOB_SW_3C_P1_A1-vlan4]desc VLAN_P1
[GOB_SW_3C_P1_A1-vlan4]vlan 5
[GOB_SW_3C_P1_A1-vlan5]name VLAN_PB
[GOB_SW_3C_P1_A1-vlan5]desc VLAN_PB
[GOB_SW_3C_P1_A1-vlan5]vlan 6
[GOB_SW_3C_P1_A1-vlan6]name TERCEROS
[GOB_SW_3C_P1_A1-vlan6]desc TERCEROS
[GOB_SW_3C_P1_A1-vlan6]vlan 7
[GOB_SW_3C_P1_A1-vlan7]name VLAN_P2
[GOB_SW_3C_P1_A1-vlan7]desc VLAN_P2
[GOB_SW_3C_P1_A1-vlan7]vlan 8
[GOB_SW_3C_P1_A1-vlan8]name VLAN_VIP
[GOB_SW_3C_P1_A1-vlan8]desc VLAN_VIP
[GOB_SW_3C_P1_A1-vlan8]
[GOB_SW_3C_P1_A1-vlan8]
```

Figura 41 Configuración de VLAN en Switch 1 P1
Elaborado por: Los autores

```
[GOB_SW_3C_P1_A1-vlan8]int ethernet 1/0/4
[GOB_SW_3C_P1_A1-Ethernet1/0/4]port link-type trunk
[GOB_SW_3C_P1_A1-Ethernet1/0/4]port trunk permit vlan all
 Please wait..... Done.
[GOB_SW_3C_P1_A1-Ethernet1/0/4]desc HACIA_GOB_SW_CS_P2_A2
[GOB_SW_3C_P1_A1-Ethernet1/0/4]
[GOB_SW_3C_P1_A1-Ethernet1/0/4]int ethernet 1/0/5
[GOB_SW_3C_P1_A1-Ethernet1/0/5]port link-type trunk
[GOB_SW_3C_P1_A1-Ethernet1/0/5]port trunk permit vlan all
 Please wait..... Done.
[GOB_SW_3C_P1_A1-Ethernet1/0/5]desc HACIA_GOB_SW_CS_PB_A2
[GOB_SW_3C_P1_A1-Ethernet1/0/5]
[GOB_SW_3C_P1_A1-Ethernet1/0/5]int ethernet 1/0/6
[GOB_SW_3C_P1_A1-Ethernet1/0/6]port link-type trunk
[GOB_SW_3C_P1_A1-Ethernet1/0/6]port trunk permit vlan all
 Please wait..... Done.
[GOB_SW_3C_P1_A1-Ethernet1/0/6]desc HACIA_GOB_SW_CS_P1_A2
```

Figura 42 Configuración de puertos modo Trunk en Switch 1 P1
Elaborado por: Los autores

```
[GOB_SW_3C_P1_A1-Ethernet1/0/6]int ethernet 1/0/1
[GOB_SW_3C_P1_A1-Ethernet1/0/1]port link-type access
[GOB_SW_3C_P1_A1-Ethernet1/0/1]port access vlan 4
[GOB_SW_3C_P1_A1-Ethernet1/0/1]
[GOB_SW_3C_P1_A1-Ethernet1/0/1]int ethernet 1/0/2
[GOB_SW_3C_P1_A1-Ethernet1/0/2]port link-type access
[GOB_SW_3C_P1_A1-Ethernet1/0/2]port access vlan 4
```

Figura 43 Configuración de puertos modo Acceso en Switch 1 P1
Elaborado por: Los autores

El Switch 2 del Piso 1 se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_P1_A2

- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/24 se estableció como puerto trunk hacía el Switch 1 del Piso 1, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
[GOB_SW_3C_P1_A2]vlan 99
[GOB_SW_3C_P1_A2-vlan99]name ADMIN
[GOB_SW_3C_P1_A2-vlan99]desc ADMIN
[GOB_SW_3C_P1_A2-vlan99]vlan 2
[GOB_SW_3C_P1_A2-vlan2]name SERVERS
[GOB_SW_3C_P1_A2-vlan2]desc SERVERS
[GOB_SW_3C_P1_A2-vlan2]vlan 3
[GOB_SW_3C_P1_A2-vlan3]name TELEFONIA
[GOB_SW_3C_P1_A2-vlan3]desc TELEFONIA
[GOB_SW_3C_P1_A2-vlan3]vlan 4
[GOB_SW_3C_P1_A2-vlan4]name VLAN_P1
[GOB_SW_3C_P1_A2-vlan4]desc VLAN_P1
[GOB_SW_3C_P1_A2-vlan4]vlan 5
[GOB_SW_3C_P1_A2-vlan5]name VLAN_PB
[GOB_SW_3C_P1_A2-vlan5]desc VLAN_PB
[GOB_SW_3C_P1_A2-vlan5]vlan 6
[GOB_SW_3C_P1_A2-vlan6]name TERCEROS
[GOB_SW_3C_P1_A2-vlan6]desc TERCEROS
[GOB_SW_3C_P1_A2-vlan6]vlan 7
[GOB_SW_3C_P1_A2-vlan7]name VLAN_P2
[GOB_SW_3C_P1_A2-vlan7]desc VLAN_P2
[GOB_SW_3C_P1_A2-vlan7]vlan 8
[GOB_SW_3C_P1_A2-vlan8]name VLAN_VIP
[GOB_SW_3C_P1_A2-vlan8]desc VLAN_VIP
[GOB_SW_3C_P1_A2-vlan8]
[GOB_SW_3C_P1_A2-vlan8]
```

Figura 44. Configuración de VLAN en Switch 2 P1
Elaborado por: Los autores

```
[GOB_SW_3C_P1_A2-Ethernet1/0/24]port link-type trunk
[GOB_SW_3C_P1_A2-Ethernet1/0/24]port trunk permit vlan all
 Please wait..................................... Done.
[GOB_SW_3C_P1_A2-Ethernet1/0/24]desc HACIA_GOB_SW_CS_P1_A1
```

Figura 45 Configuración de puertos modo Trunk en Switch 2 P1
Elaborado por: Los autores

```
[GOB_SW_3C_P1_A2-Ethernet1/0/24]
[GOB_SW_3C_P1_A2-Ethernet1/0/24]int ethernet 1/0/1
[GOB_SW_3C_P1_A2-Ethernet1/0/1]port link-type access
[GOB_SW_3C_P1_A2-Ethernet1/0/1]port access vlan 4
[GOB_SW_3C_P1_A2-Ethernet1/0/1]
[GOB_SW_3C_P1_A2-Ethernet1/0/1]int ethernet 1/0/2
[GOB_SW_3C_P1_A2-Ethernet1/0/2]port link-type access
[GOB_SW_3C_P1_A2-Ethernet1/0/2]port access vlan 4
```

Figura 46 Configuración de puertos modo Acceso en Switch 2 P1
Elaborado por: Los autores

El Switch 1 de Planta Baja se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_PB_A1
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/49 se estableció como puerto trunk hacía el Switch 2 del Piso 2, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
[GOB]sysname GOB_SW_3C_PB_A1
[GOB_SW_3C_PB_A1]vlan 99
[GOB_SW_3C_PB_A1-vlan99]name ADMIN
[GOB_SW_3C_PB_A1-vlan99]desc ADMIN
[GOB_SW_3C_PB_A1-vlan99]vlan 2
[GOB_SW_3C_PB_A1-vlan2]name SERVERS
[GOB_SW_3C_PB_A1-vlan2]desc SERVERS
[GOB_SW_3C_PB_A1-vlan2]vlan 3
[GOB_SW_3C_PB_A1-vlan3]name TELEFONIA
[GOB_SW_3C_PB_A1-vlan3]desc TELEFONIA
[GOB_SW_3C_PB_A1-vlan3]vlan 4
[GOB_SW_3C_PB_A1-vlan4]name VLAN_P1
[GOB_SW_3C_PB_A1-vlan4]desc VLAN_P1
[GOB_SW_3C_PB_A1-vlan4]vlan 5
[GOB_SW_3C_PB_A1-vlan5]name VLAN_PB
[GOB_SW_3C_PB_A1-vlan5]desc VLAN_PB
[GOB_SW_3C_PB_A1-vlan5]vlan 6
[GOB_SW_3C_PB_A1-vlan6]name TERCEROS
[GOB_SW_3C_PB_A1-vlan6]desc TERCEROS
[GOB_SW_3C_PB_A1-vlan6]vlan 7
[GOB_SW_3C_PB_A1-vlan7]name VLAN_P2
[GOB_SW_3C_PB_A1-vlan7]desc VLAN_P2
[GOB_SW_3C_PB_A1-vlan7]vlan 8
[GOB_SW_3C_PB_A1-vlan8]name VLAN_VIP
[GOB_SW_3C_PB_A1-vlan8]desc VLAN_VIP
[GOB_SW_3C_PB_A1-vlan8]
[GOB_SW_3C_PB_A1-vlan8]
```

Figura 47 Configuración de VLAN en Switch 1 PB
Elaborado por: Los autores

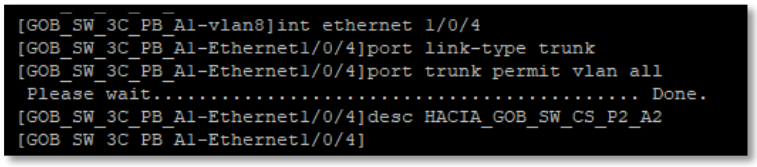


Figura 48 Configuración de puertos modo Trunk en Switch 1 PB
Elaborado por: Los autores

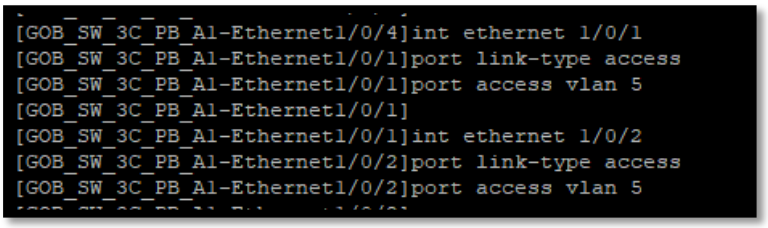


Figura 49 Configuración de puertos modo Acceso en Switch 1 PB
Elaborado por: Los autores

El Switch 2 de Planta Baja se configuró de la siguiente forma:

- Se cambió el nombre del dispositivo de acuerdo con la tabla 29: GOB_SW_3C_PB_A2
- Se añadieron todas las VLAN de acuerdo con el ID y nombre acordado en la tabla 28.
- El puerto 1/0/16 se estableció como puerto trunk hacía el Switch 1 del Piso 1, permitiendo el paso de las VLAN correspondientes.
- De acuerdo con el departamento donde se encuentra el punto se configuró la VLAN correspondiente en modo acceso.
- Y demás configuraciones de acuerdo con la tabla 30.

```
[gob]sysname GOB_SW_3C_PB_A2
[GOB_SW_3C_PB_A2]vlan 99
[GOB_SW_3C_PB_A2-vlan99]name ADMIN
[GOB_SW_3C_PB_A2-vlan99]desc ADMIN
[GOB_SW_3C_PB_A2-vlan99]vlan 2
[GOB_SW_3C_PB_A2-vlan2]name SERVERS
[GOB_SW_3C_PB_A2-vlan2]desc SERVERS
[GOB_SW_3C_PB_A2-vlan2]vlan 3
[GOB_SW_3C_PB_A2-vlan3]name TELEFONIA
[GOB_SW_3C_PB_A2-vlan3]desc TELEFONIA
[GOB_SW_3C_PB_A2-vlan3]vlan 4
[GOB_SW_3C_PB_A2-vlan4]name VLAN_P1
[GOB_SW_3C_PB_A2-vlan4]desc VLAN_P1
[GOB_SW_3C_PB_A2-vlan4]vlan 5
[GOB_SW_3C_PB_A2-vlan5]name VLAN_PB
[GOB_SW_3C_PB_A2-vlan5]desc VLAN_PB
[GOB_SW_3C_PB_A2-vlan5]vlan 6
[GOB_SW_3C_PB_A2-vlan6]name TERCEROS
[GOB_SW_3C_PB_A2-vlan6]desc TERCEROS
[GOB_SW_3C_PB_A2-vlan6]vlan 7
[GOB_SW_3C_PB_A2-vlan7]name VLAN_P2
[GOB_SW_3C_PB_A2-vlan7]desc VLAN_P2
[GOB_SW_3C_PB_A2-vlan7]vlan 8
[GOB_SW_3C_PB_A2-vlan8]name VLAN_VIP
[GOB_SW_3C_PB_A2-vlan8]desc VLAN_VIP
[GOB_SW_3C_PB_A2-vlan8]
[GOB_SW_3C_PB_A2-vlan8]
```

Figura 50 Configuración de VLAN en Switch 2 PB
Elaborado por: Los autores

```
[GOB_SW_3C_PB_A2-vlan8]int ethernet 1/0/16
[GOB_SW_3C_PB_A2-Ethernet1/0/16]port link-type trunk
[GOB_SW_3C_PB_A2-Ethernet1/0/16]port trunk permit vlan all
 Please wait..... Done.
[GOB_SW_3C_PB_A2-Ethernet1/0/16]desc HACIA_GOB_SW_CS_P1_A1
```

Figura 51 Configuración de puertos modo Trunk en Switch 2 PB
Elaborado por: Los autores

```
[GOB_SW_3C_PB_A2-Ethernet1/0/16]int ethernet 1/0/1
[GOB_SW_3C_PB_A2-Ethernet1/0/1]port link-type access
[GOB_SW_3C_PB_A2-Ethernet1/0/1]port access vlan 5
[GOB_SW_3C_PB_A2-Ethernet1/0/1]
[GOB_SW_3C_PB_A2-Ethernet1/0/1]int ethernet 1/0/2
[GOB_SW_3C_PB_A2-Ethernet1/0/2]port link-type access
[GOB_SW_3C_PB_A2-Ethernet1/0/2]port access vlan 5
```

Figura 52 Configuración de puertos modo Acceso en Switch 2 PB
Elaborado por: Los autores

5.4.2. Configuración de VLAN en Access Points

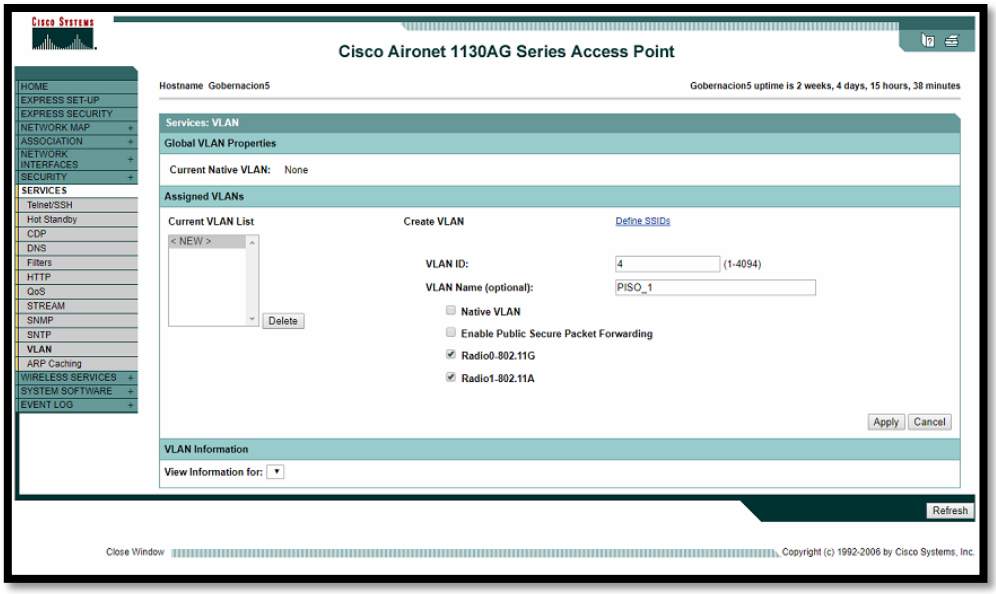


Figura 53 Configuración de VLAN del piso en AP Piso 1
Elaborado por: Los autores

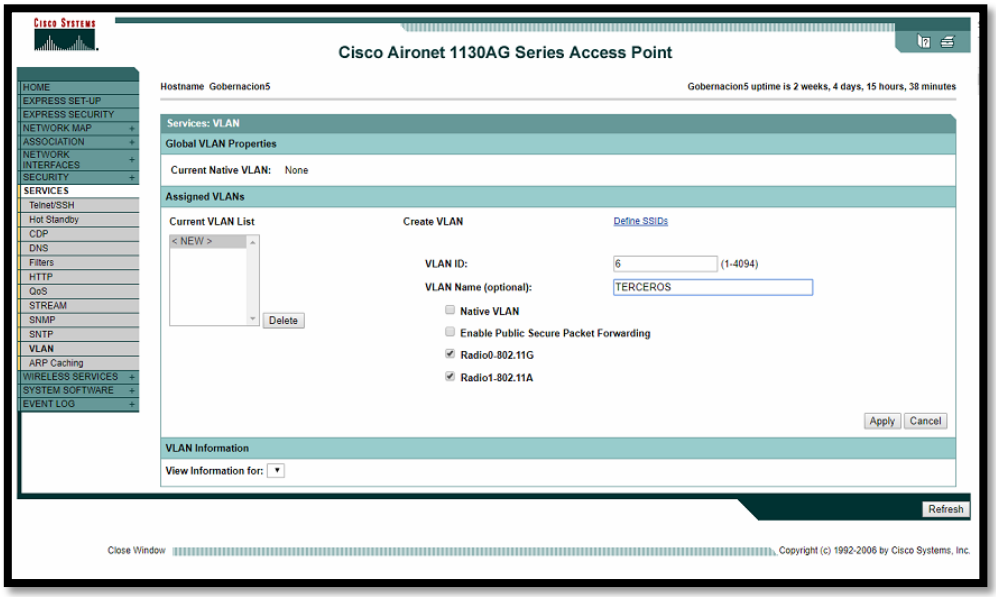


Figura 54 Configuración de VLAN Terceros en AP Piso 1
Elaborado por: Los autores

Figura 55 Configuración de VLAN VIP en AP Piso 1
Elaborado por: Los autores

5.4.3. Configuración de directorio activo

Se instaló y configuró el servidor de dominio en un servidor con Windows Server 2008 R2, el proceso de instalación y configuraciones se encuentra en el **Anexo C**, a continuación, se detallará el resultado de cada configuración.

Se creó un dominio con el nombre "GoberGuayas.local" en el cual se crearon dos unidades directivas, "Equipos" y "Usuarios", dentro de las mismas se definieron los equipos y usuarios acorde a cada departamento.

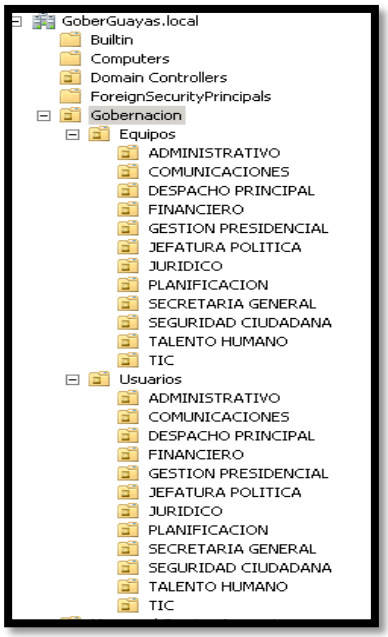


Figura 56. Dominio, unidades organizativas y departamentos.
Elaborado por: Los autores

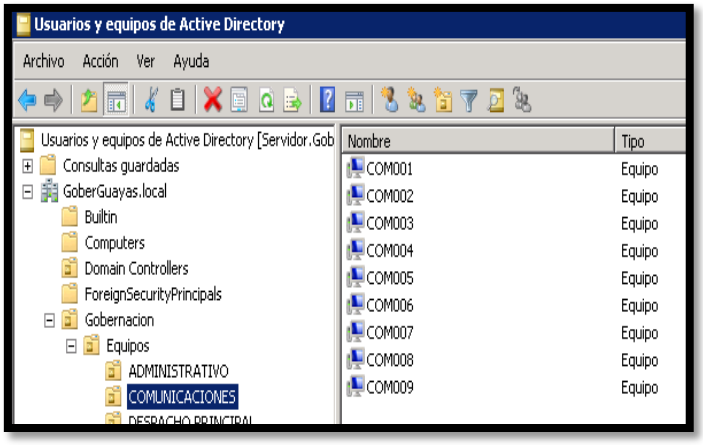


Figura 57. Equipos configurados por departamento.
Elaborado por: Los autores

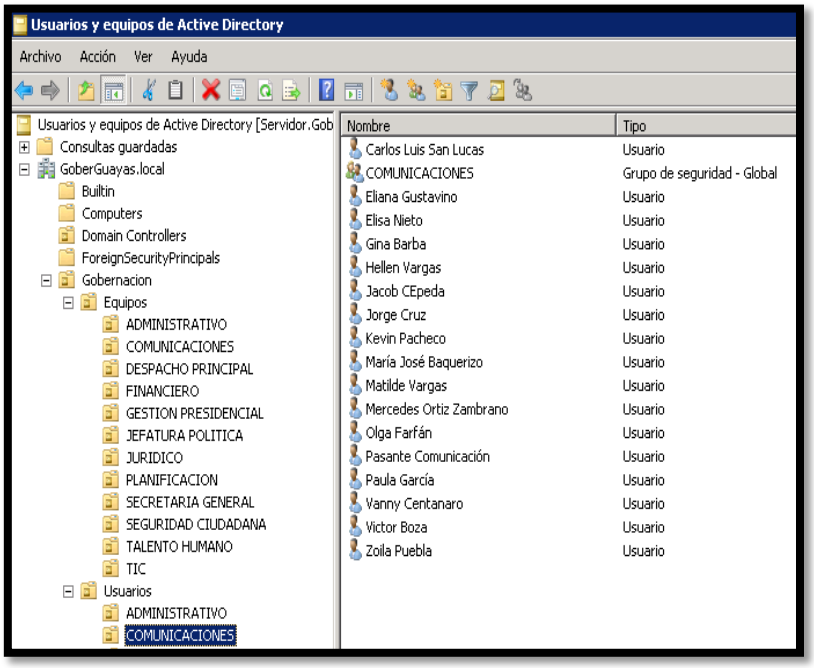


Figura 58. Usuarios y grupo de seguridad configurado por departamento.
Elaborado por: Los autores.

Se crearon las directivas de dominio por defecto que será la primera barrera de políticas dispuesta por la institución hacia los usuarios.

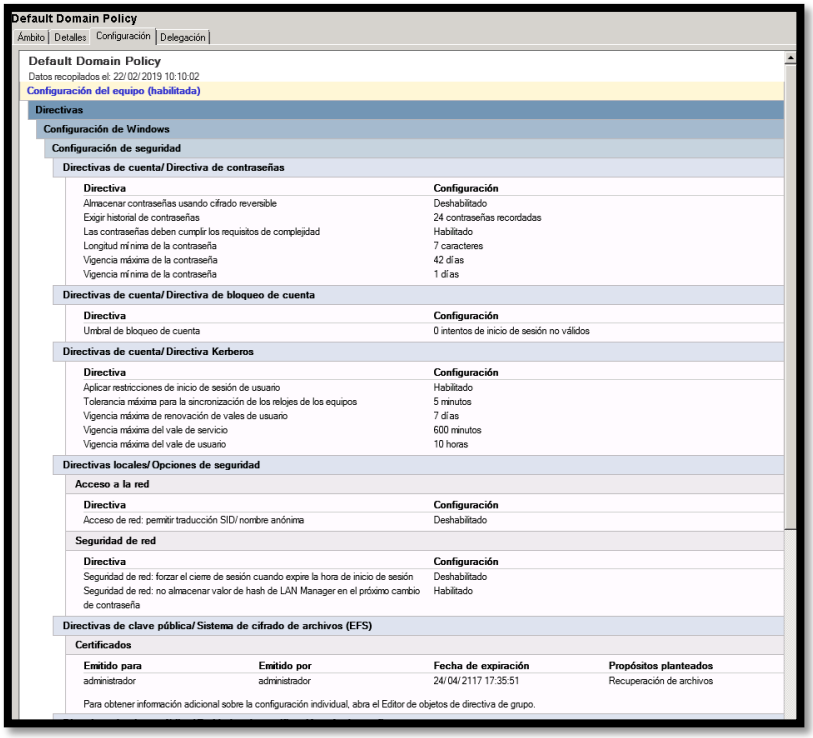


Figura 59. Directivas por defecto para el equipo.
Elaborado por: Los autores.

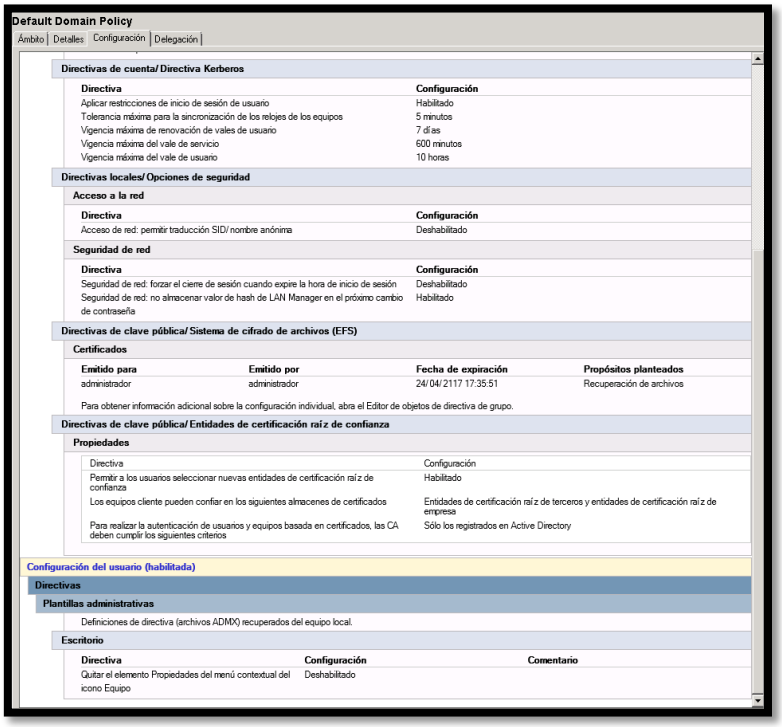
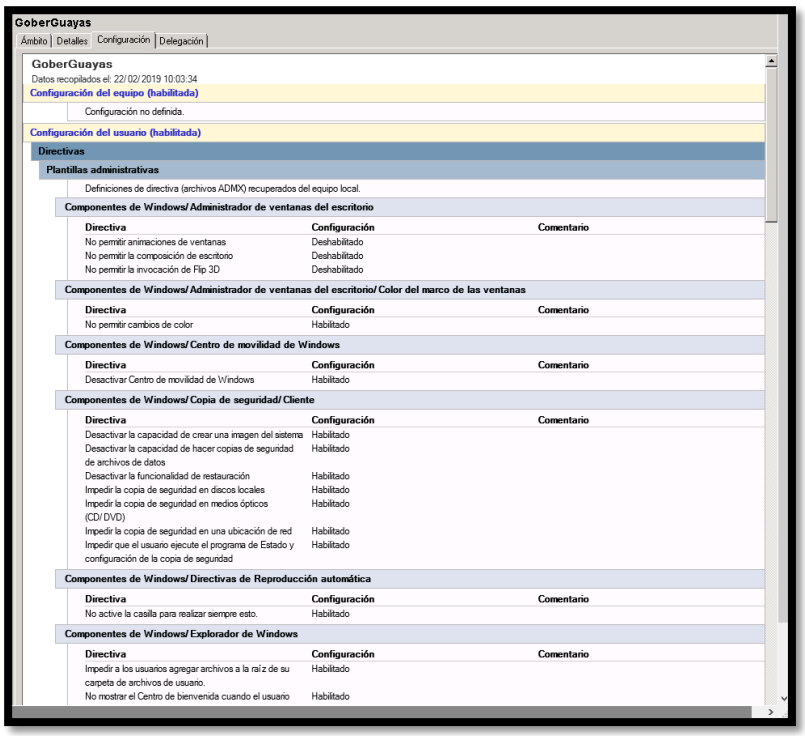


Figura 60. Directivas por defecto de equipo y usuario.
Elaborado por: Los autores

Así mismo se crearon directivas bajo el nombre “GoberGuayas”, dichas políticas fueron definidas por la institución.


GoberGuayas

Ámbito | Detalles | Configuración | Delegación |

GoberGuayas

Datos recopilados el: 22/02/2019 10:03:34

Configuración del equipo (habilitada)

Configuración no definida.

Configuración del usuario (habilitada)

Directivas

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperados del equipo local.

Componentes de Windows/ Administrador de ventanas del escritorio

Directiva	Configuración	Comentario
No permitir animaciones de ventanas	Deshabilitado	
No permitir la composición de escritorio	Deshabilitado	
No permitir la invocación de Flip 3D	Deshabilitado	

Componentes de Windows/ Administrador de ventanas del escritorio/ Color del marco de las ventanas

Directiva	Configuración	Comentario
No permitir cambios de color	Habilitado	

Componentes de Windows/ Centro de movilidad de Windows

Directiva	Configuración	Comentario
Desactivar Centro de movilidad de Windows	Habilitado	

Componentes de Windows/ Copia de seguridad/ Cliente

Directiva	Configuración	Comentario
Desactivar la capacidad de crear una imagen del sistema	Habilitado	
Desactivar la capacidad de hacer copias de seguridad de archivos de datos	Habilitado	
Desactivar la funcionalidad de restauración	Habilitado	
Impedir la copia de seguridad en discos locales	Habilitado	
Impedir la copia de seguridad en medios ópticos (CD/DVD)	Habilitado	
Impedir la copia de seguridad en una ubicación de red	Habilitado	
Impedir que el usuario ejecute el programa de Estado y configuración de la copia de seguridad	Habilitado	

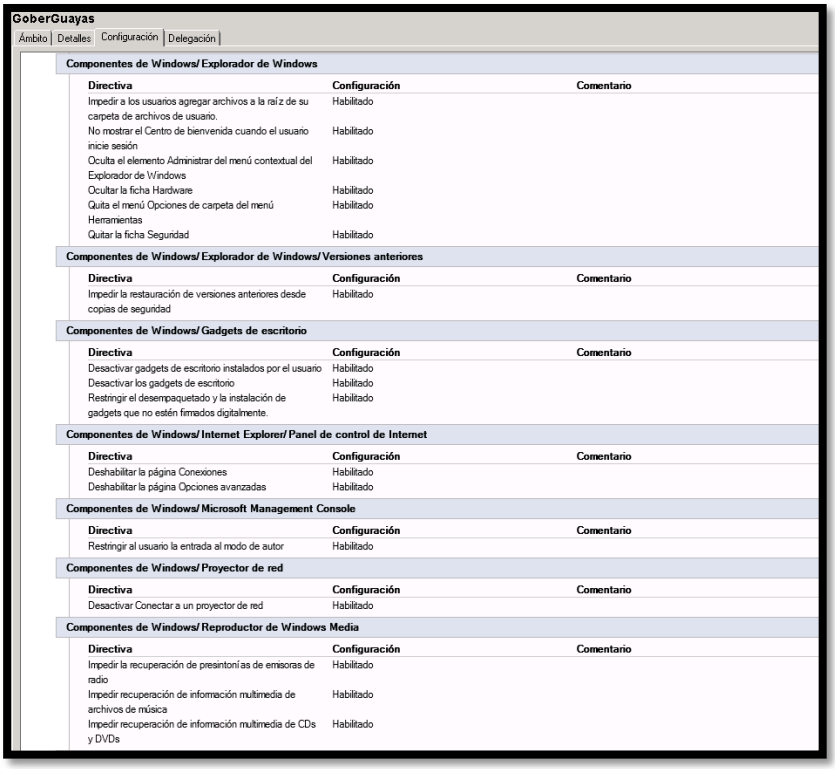
Componentes de Windows/ Directivas de Reproducción automática

Directiva	Configuración	Comentario
No active la casilla para realizar siempre esto.	Habilitado	

Componentes de Windows/ Explorador de Windows

Directiva	Configuración	Comentario
Impedir a los usuarios agregar archivos a la raíz de su carpeta de archivos de usuario.	Habilitado	
No mostrar el Centro de bienvenida cuando el usuario	Habilitado	

Figura 61. Directivas para usuarios.
Elaborado por: Los autores


GoberGuayas

Ámbito | Detalles | Configuración | Delegación |

Componentes de Windows/ Explorador de Windows

Directiva	Configuración	Comentario
Impedir a los usuarios agregar archivos a la raíz de su carpeta de archivos de usuario.	Habilitado	
No mostrar el Centro de bienvenida cuando el usuario inicie sesión	Habilitado	
Oculta el elemento Administrar del menú contextual del Explorador de Windows	Habilitado	
Ocultar la ficha Hardware	Habilitado	
Quita el menú Opciones de carpeta del menú Herramientas	Habilitado	
Quitar la ficha Seguridad	Habilitado	

Componentes de Windows/ Explorador de Windows/ Versiones anteriores

Directiva	Configuración	Comentario
Impedir la restauración de versiones anteriores desde copias de seguridad	Habilitado	

Componentes de Windows/ Gadgets de escritorio

Directiva	Configuración	Comentario
Desactivar gadgets de escritorio instalados por el usuario	Habilitado	
Desactivar los gadgets de escritorio	Habilitado	
Restringir el desempaquetado y la instalación de gadgets que no estén firmados digitalmente.	Habilitado	

Componentes de Windows/ Internet Explorer/ Panel de control de Internet

Directiva	Configuración	Comentario
Deshabilitar la página Conexiones	Habilitado	
Deshabilitar la página Opciones avanzadas	Habilitado	

Componentes de Windows/ Microsoft Management Console

Directiva	Configuración	Comentario
Restringir al usuario la entrada al modo de autor	Habilitado	

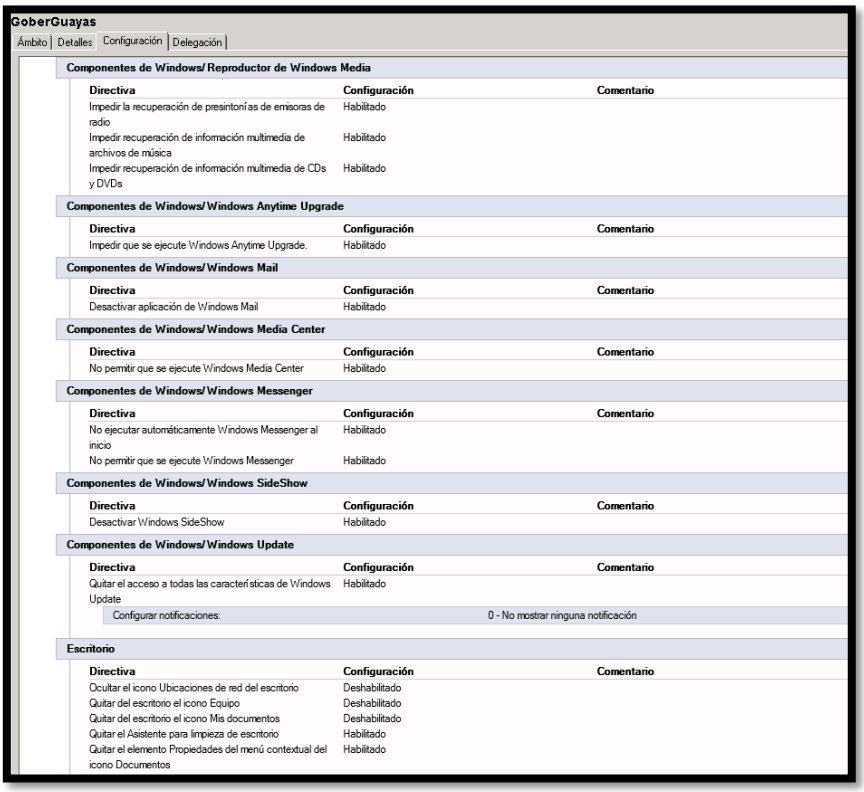
Componentes de Windows/ Proyector de red

Directiva	Configuración	Comentario
Desactivar Conectar a un proyector de red	Habilitado	

Componentes de Windows/ Reproductor de Windows Media

Directiva	Configuración	Comentario
Impedir la recuperación de presintonías de emisoras de radio	Habilitado	
Impedir recuperación de información multimedia de archivos de música	Habilitado	
Impedir recuperación de información multimedia de CDs y DVDs	Habilitado	

Figura 62. Directivas de usuarios.
Elaborado por: Los autores



GoberGuayas

Ámbito | Detalles | Configuración | Delegación |

Componentes de Windows/ Reproductor de Windows Media

Directiva	Configuración	Comentario
Impedir la recuperación de presintoní as de emisoras de radio	Habilitado	
Impedir recuperación de información multimedia de archivos de música	Habilitado	
Impedir recuperación de información multimedia de CDs y DVDs	Habilitado	

Componentes de Windows/ Windows Anytime Upgrade

Directiva	Configuración	Comentario
Impedir que se ejecute Windows Anytime Upgrade.	Habilitado	

Componentes de Windows/ Windows Mail

Directiva	Configuración	Comentario
Desactivar aplicación de Windows Mail	Habilitado	

Componentes de Windows/ Windows Media Center

Directiva	Configuración	Comentario
No permitir que se ejecute Windows Media Center	Habilitado	

Componentes de Windows/ Windows Messenger

Directiva	Configuración	Comentario
No ejecutar automáticamente Windows Messenger al inicio	Habilitado	
No permitir que se ejecute Windows Messenger	Habilitado	

Componentes de Windows/ Windows SideShow

Directiva	Configuración	Comentario
Desactivar Windows SideShow	Habilitado	

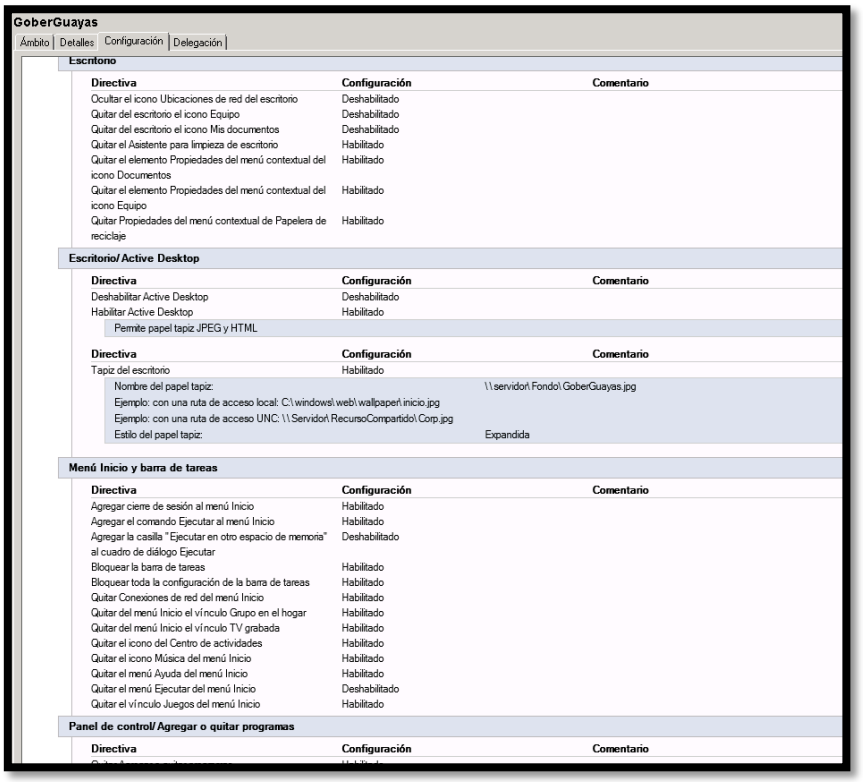
Componentes de Windows/ Windows Update

Directiva	Configuración	Comentario
Quitar el acceso a todas las caracterí sticas de Windows Update	Habilitado	
Configurar notificaciones:	0 - No mostrar ninguna notificación	

Escritorio

Directiva	Configuración	Comentario
Ocultar el icono Ubicaciones de red del escritorio	Deshabilitado	
Quitar del escritorio el icono Equipo	Deshabilitado	
Quitar del escritorio el icono Mis documentos	Deshabilitado	
Quitar el Asistente para limpieza de escritorio	Habilitado	
Quitar el elemento Propiedades del menú contextual del icono Documentos	Habilitado	

Figura 63. Directivas de usuarios.
Elaborado por: Los autores



GoberGuayas

Ámbito | Detalles | Configuración | Delegación |

Escritorio

Directiva	Configuración	Comentario
Ocultar el icono Ubicaciones de red del escritorio	Deshabilitado	
Quitar del escritorio el icono Equipo	Deshabilitado	
Quitar del escritorio el icono Mis documentos	Deshabilitado	
Quitar el Asistente para limpieza de escritorio	Habilitado	
Quitar el elemento Propiedades del menú contextual del icono Documentos	Habilitado	
Quitar el elemento Propiedades del menú contextual del icono Equipo	Habilitado	
Quitar Propiedades del menú contextual de Papelera de reciclaje	Habilitado	

Escritorio/ Active Desktop

Directiva	Configuración	Comentario
Deshabilitar Active Desktop	Deshabilitado	
Habilitar Active Desktop	Habilitado	
Permite papel tapiz JPEG y HTML		

Directiva	Configuración	Comentario
Tapiz del escritorio	Habilitado	
Nombre del papel tapiz:	\\servidor\ Fondo\ GoberGuayas.jpg	
Ejemplo: con una ruta de acceso local: C:\ windows\ web\ wallpaper\ inicio.jpg		
Ejemplo: con una ruta de acceso UNC: \\ Servidor\ RecursoCompartido\ Corp.jpg		
Estilo del papel tapiz:	Expandida	

Menú Inicio y barra de tareas

Directiva	Configuración	Comentario
Agregar cierre de sesión al menú Inicio	Habilitado	
Agregar el comando Ejecutar al menú Inicio	Habilitado	
Agregar la casilla "Ejecutar en otro espacio de memoria" al cuadro de diálogo Ejecutar	Deshabilitado	
Bloquear la barra de tareas	Habilitado	
Bloquear toda la configuración de la barra de tareas	Habilitado	
Quitar Conexiones de red del menú Inicio	Habilitado	
Quitar del menú Inicio el vínculo Grupo en el hogar	Habilitado	
Quitar del menú Inicio el vínculo TV grabada	Habilitado	
Quitar el icono del Centro de actividades	Habilitado	
Quitar el icono Música del menú Inicio	Habilitado	
Quitar el menú Ayuda del menú Inicio	Habilitado	
Quitar el menú Ejecutar del menú Inicio	Deshabilitado	
Quitar el vínculo Juegos del menú Inicio	Habilitado	

Panel de control/ Agregar o quitar programas

Directiva	Configuración	Comentario

Figura 64. Directivas de usuarios
Elaborado por: Los autores

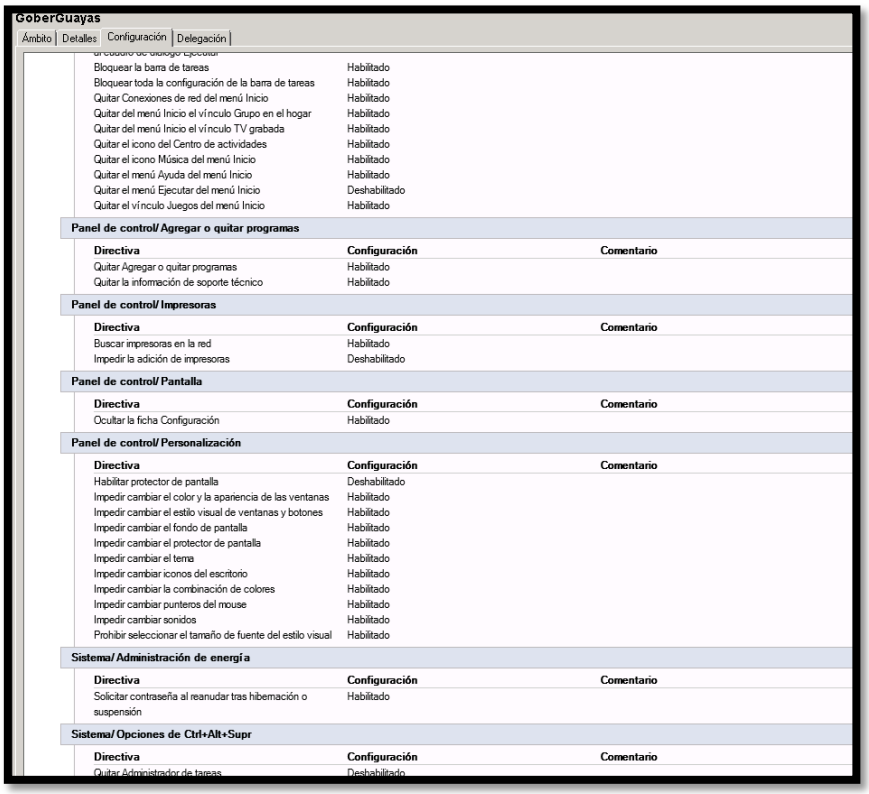


Figura 65. Directivas de usuarios.
Elaborado por: Los autores

5.4.4. Configuración de Sophos SG 210

Se instaló y configuró el Firewall UTM, el proceso de instalación y configuraciones se encuentra en el **anexo D**, a continuación, se detallará la configuración de los siguientes módulos:

- Management

  - **Shell Access**

Se configuró las redes que tendrán acceso vía SSH y el puerto por el que se conectarán.

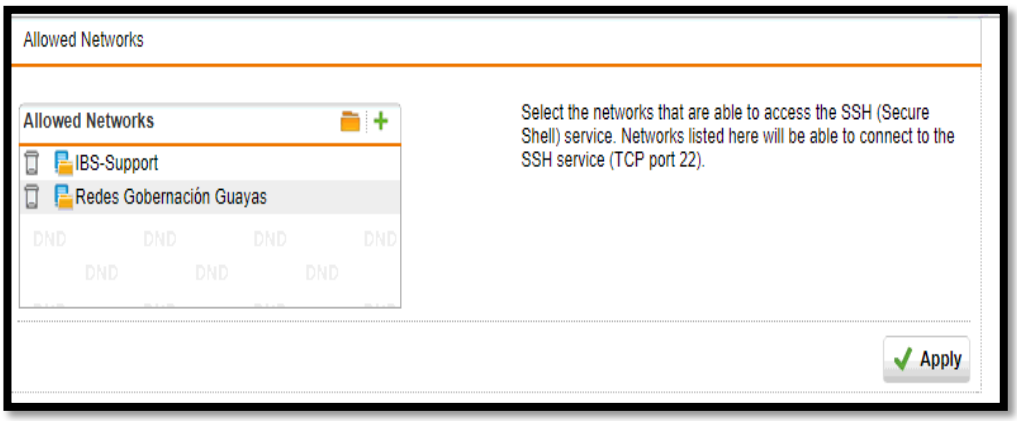


Figura 66. Redes permitidas para conexión SSH en Sophos.
Elaborado por: Los autores

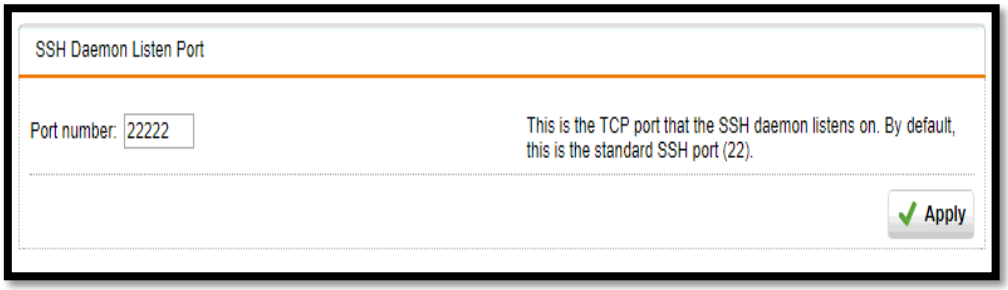


Figura 67. Puerto de escucha para SSH en Sophos.
Elaborado por: Los autores

- **Backup/Restore**

En este apartado se configuró el equipo para que realice respaldos diarios y que máximo almacene hasta 10 respaldos, se notificará por medio de correo al administrador.

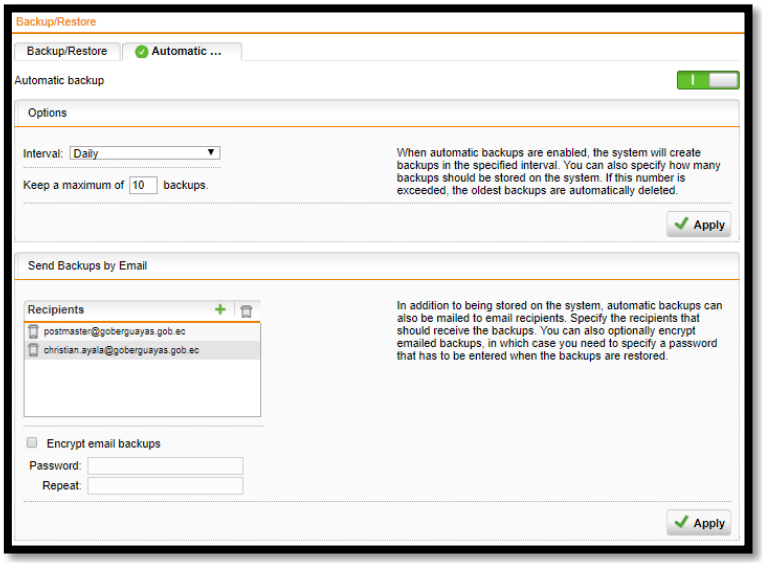


Figura 68. Backup/Restore de Sophos
Elaborado por: Los autores.

- **User Portal**

Para las diferentes actividades a realizar cuando los usuarios accedan se utiliza el puerto: 20443, al portal se le habilita la red “Cualquiera”.

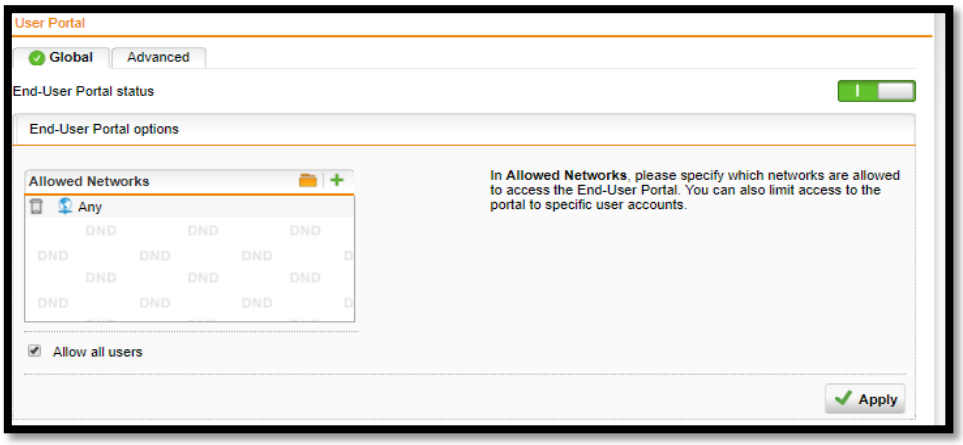


Figura 69. User portal de Sophos.
Elaborado por: Los autores.

- **Notifications**

Se configuró los correos a los que el equipo notificará eventos dentro de la red.

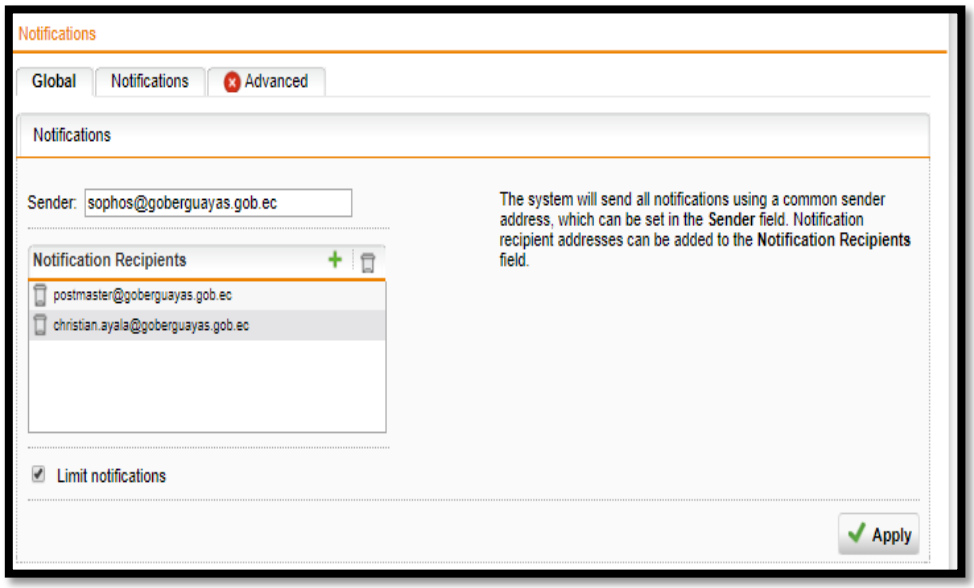


Figura 70. Notificaciones de Sophos.
Elaborado por: Los autores.

- **Central Management**

Se configuró para que el proveedor del equipo brinde el respectivo soporte: administración, monitoreo, configuración y enviar reportes de los equipos.

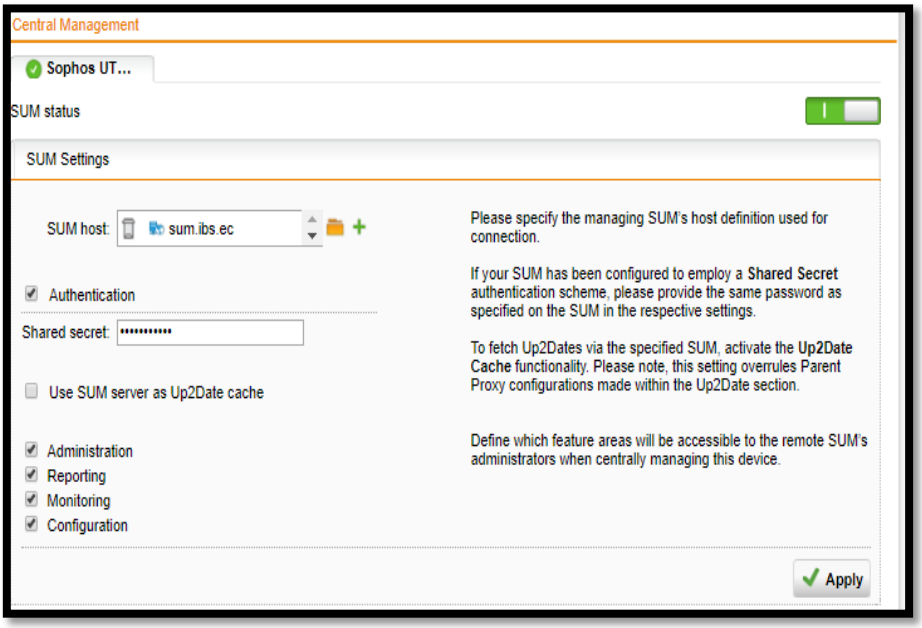


Figura 71. Central management de Sophos.
Elaborado por: Los autores.

- **Definition & Users**
  - **Network definitions**

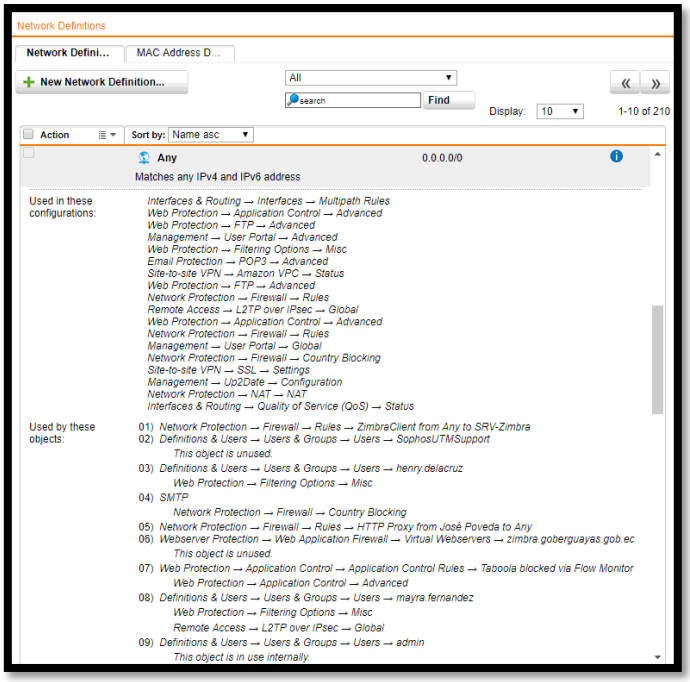


Figura 72. Definición de reglas para la red en Sophos.
Elaborado por: Los autores.

- **Service definition**

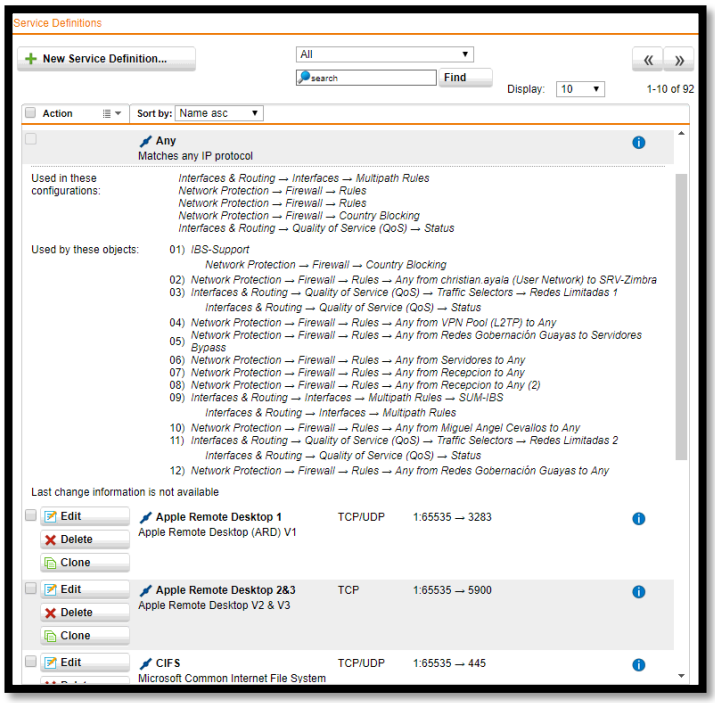


Figura 73. Definición de reglas para los servicios de red en Sophos. Elaborado por: Los autores.

- **Time period definition**

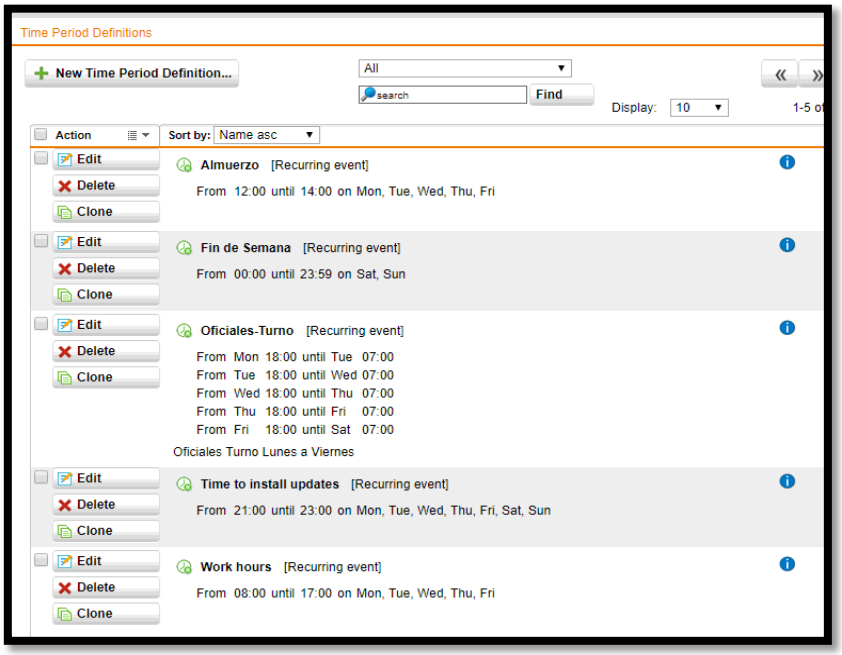


Figura 74. Definición de periodos de tiempo para uso de la red en Sophos. Elaborado por: Los autores.

- **Network Services**
  - **DNS**

Se configuró las redes a las que se le permitirá usar el sistema como DNS que resolverá de manera recursiva, dentro del mismo modulo se configuraron los DNS forwarders y el dominio local.

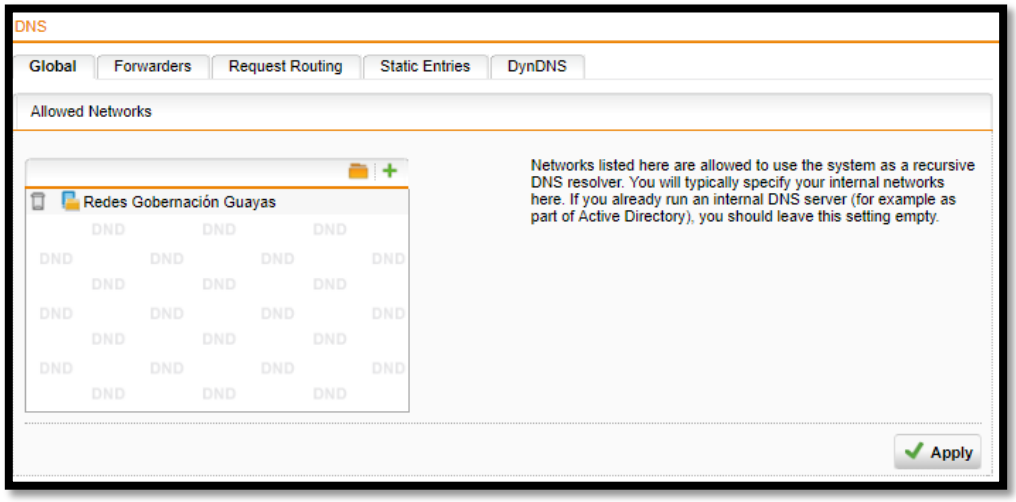


Figura 75. Redes habilitadas para DNS en Sophos.
Elaborado por: Los autores.

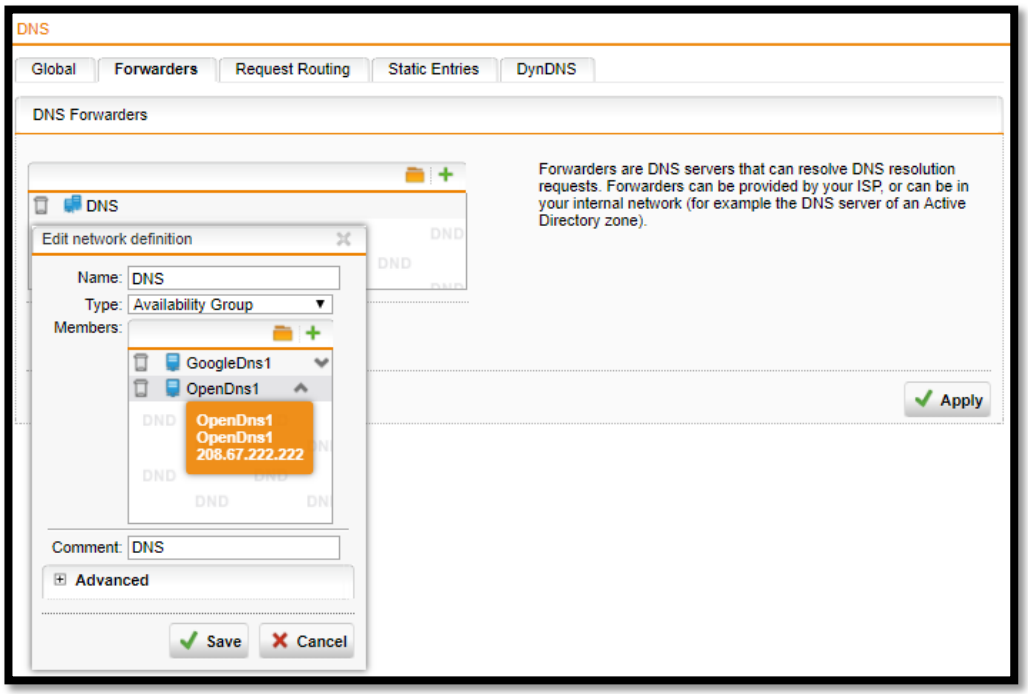


Figura 76. DNS Forwarders en Sophos.
Elaborado por: Los autores.

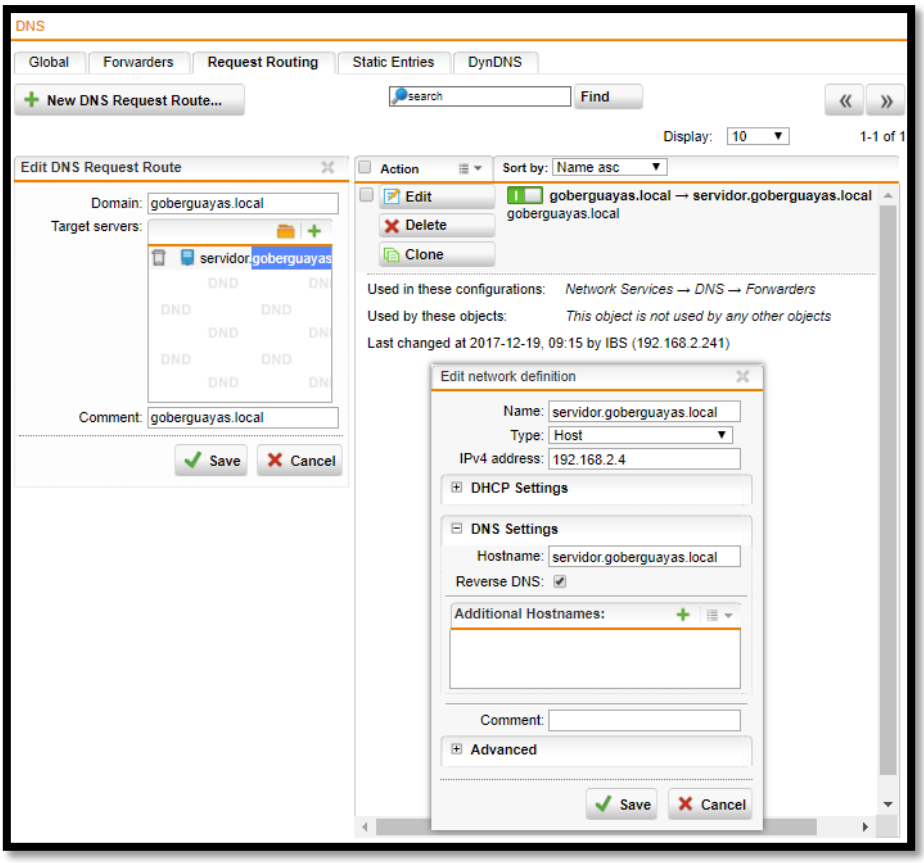


Figura 77. Dominio local DNS en Sophos.
Elaborado por: Los autores.

- **DHCP**

Se configuró el rango de IP's que se resolverán por medio de DHCP, mismas que son utilizadas para las conexiones inalámbricas.

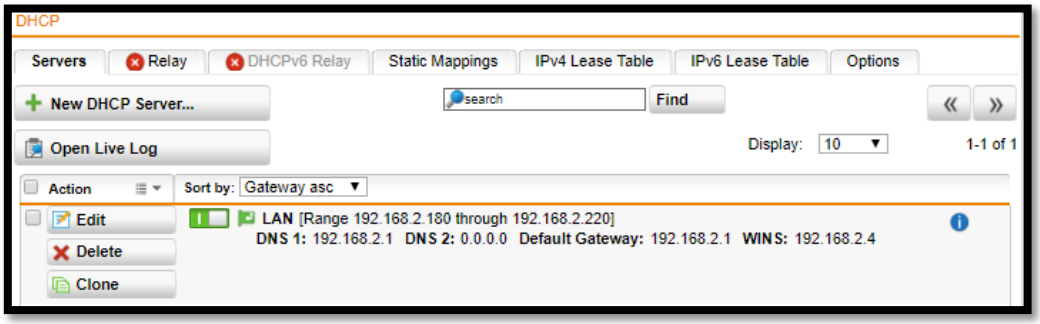


Figura 78. Rango DHCP configurado en Sophos.
Elaborado por: Los autores.

- **Network Protection**
    - **Firewall**

Se configuró este modulo que controlará el acceso de los dispositivos que usan como Gateway el UTM. La política por defecto del firewall es bloquear todo el tráfico.

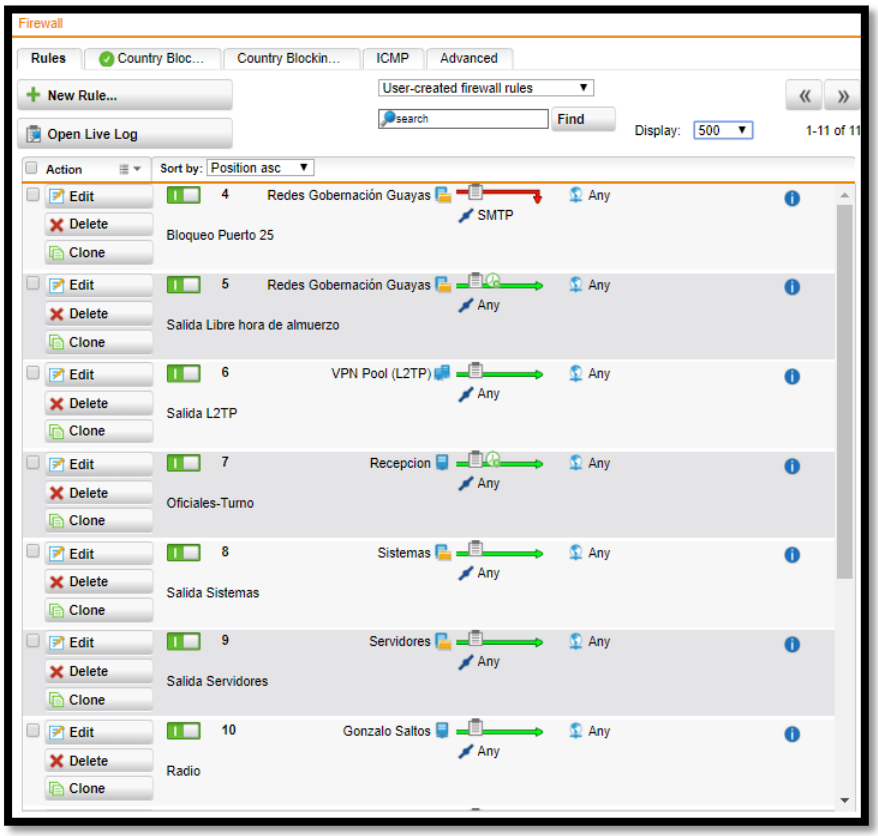


Figura 79. Reglas de Firewall en Sophos
Elaborado por: Los autores.

Se implementó la funcionalidad Country blocking, para denegar la comunicación desde lugares que no se encuentren autorizados para acceder a la infraestructura institucional. Por defecto se encuentran bloqueadas las conexiones desde todos los países a excepción de Ecuador.

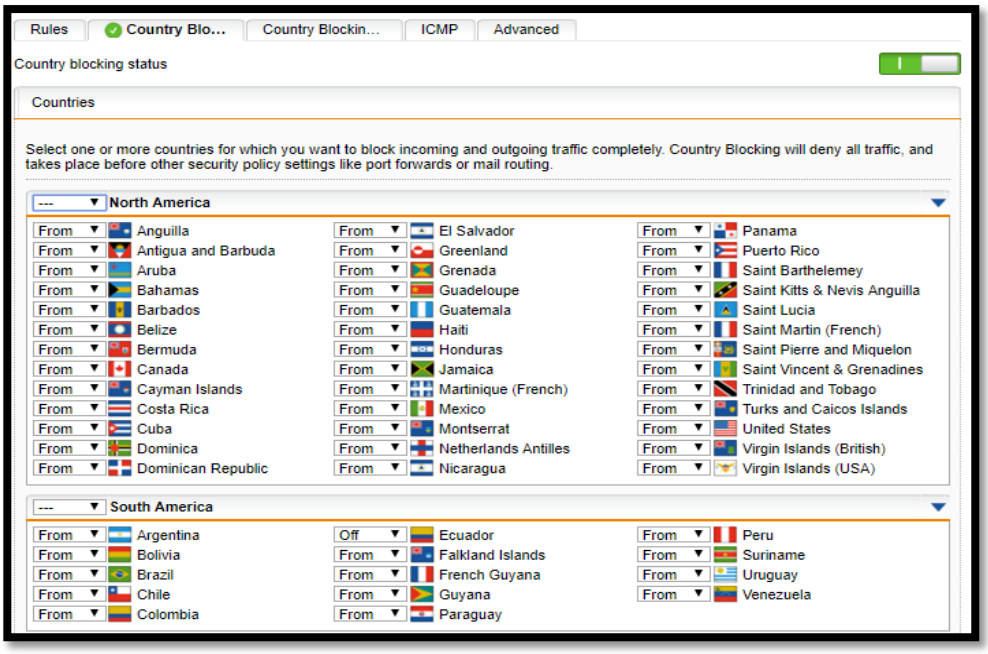


Figura 80. Country blocking en Sophos.
Elaborado por: Los autores.

- **NAT**

Se configuró la funcionalidad masquerading, misma que permite el enmascaramiento de las redes internas para poder navegar en internet, y poder hacer la transformación de IP's privadas, utilizando las IP's públicas del proveedor del servicio de internet.

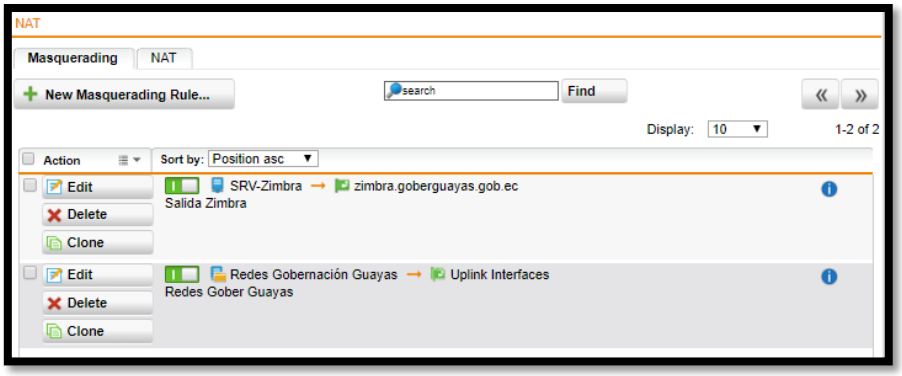


Figura 81.Masquerading en Sophos.
Elaborado por: Los autores.

En la funcionalidad NAT se configuró los redireccionamiento de puertos para que puedan acceder a los diferentes servicios institucionales.

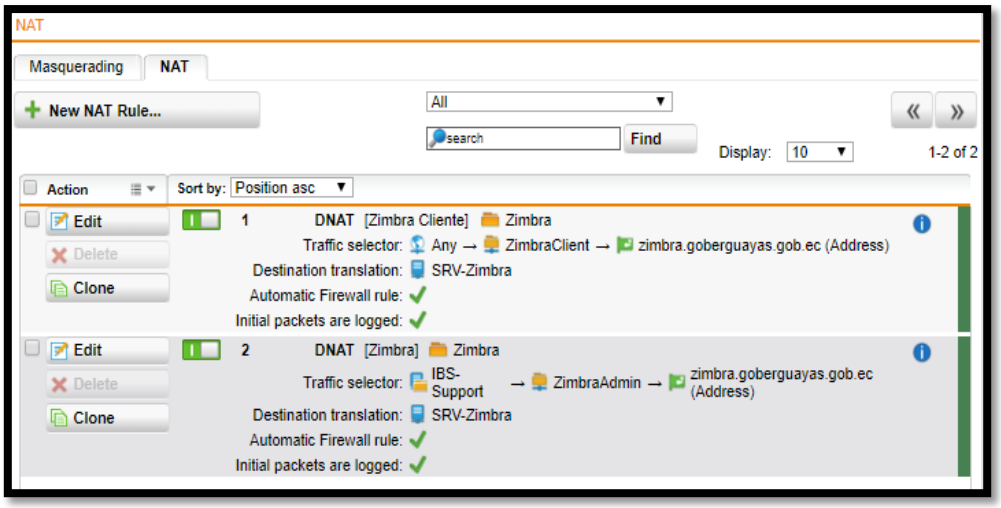


Figura 82. Configuración de NAT en Sophos.
Elaborado por: Los autores.

- **VoIP**

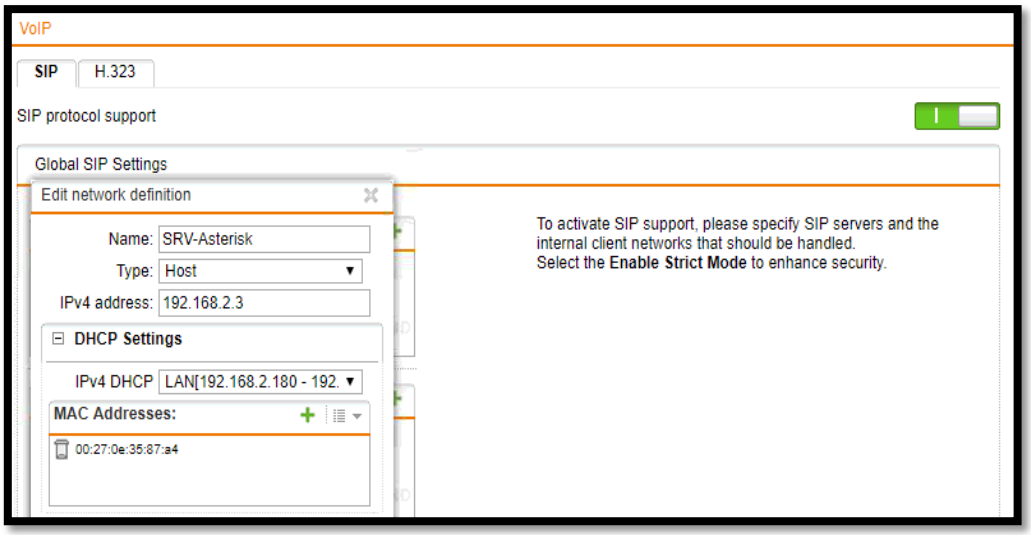


Figura 83. Configuración de Asterisk en Sophos.
Elaborado por: Los autores.

- **Web Protection**

Se configuró este módulo para el control de la navegación WEB, tanto por http (puerto 80), como en https (puerto 443). La política configurada por defecto es bloquear todo lo que no se encuentre en ningún perfil de navegación y para esto fueron creados diferentes perfiles acordes a los usuarios.

- **Web Filter Profile**

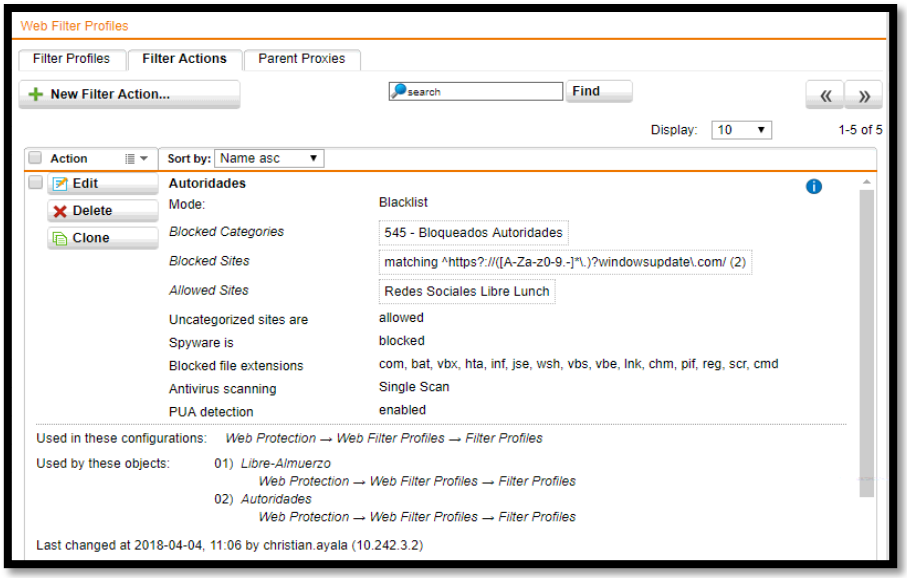


Figura 84. Descripción de un perfil de filtrado web en Sophos.
Elaborado por: Los autores.

- **Aplication Controlº**

Se configuró para tener un filtro a nivel de capa 7 sobre el acceso de los usuarios a los servicios de internet. Si bien es cierto Web Protection controla la navegación, no permite bloquear aplicaciones específicas que no corren en los navegadores.

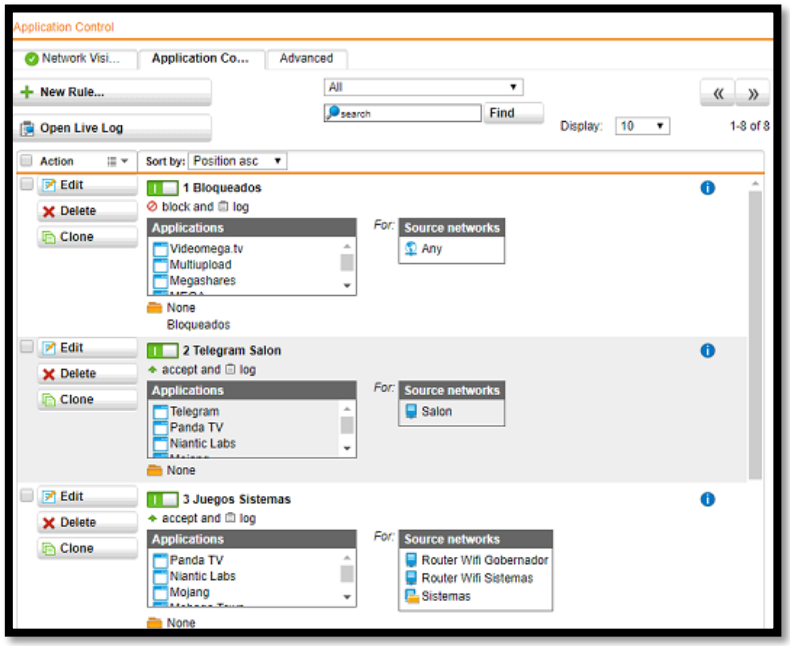


Figura 85. Bloqueo de aplicaciones en Sophos.
Elaborado por: Los autores.

- **Email Protection**
  - **SMTP**

Se configuró para que sea la primera barrera de verificación de correos antes de ser despachados.

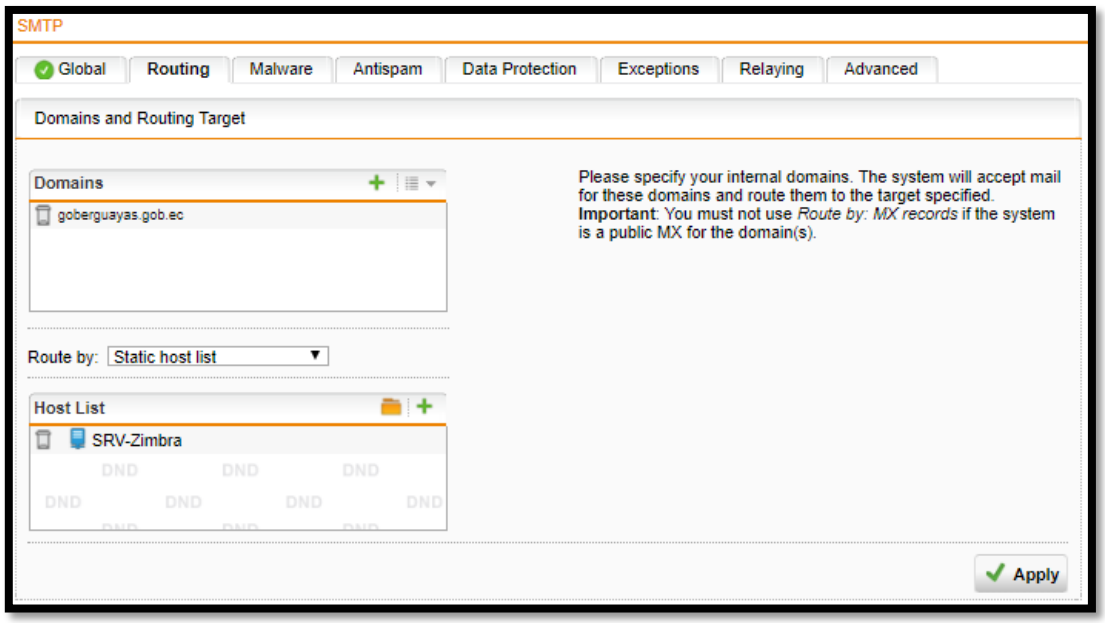


Figura 86. Configuración de dominio y ruta SMTP en Sophos.
Elaborado por: Los autores.

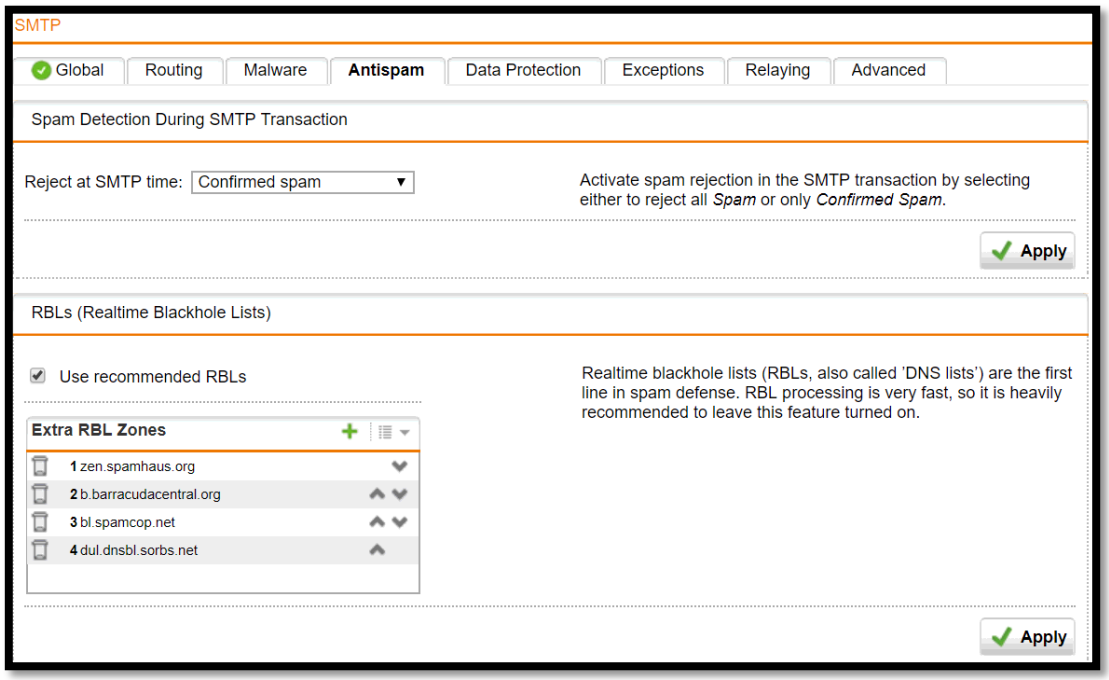


Figura 87. Configuración de Lista RBL en el Antispam de Sophos.
Elaborado por: Los autores.

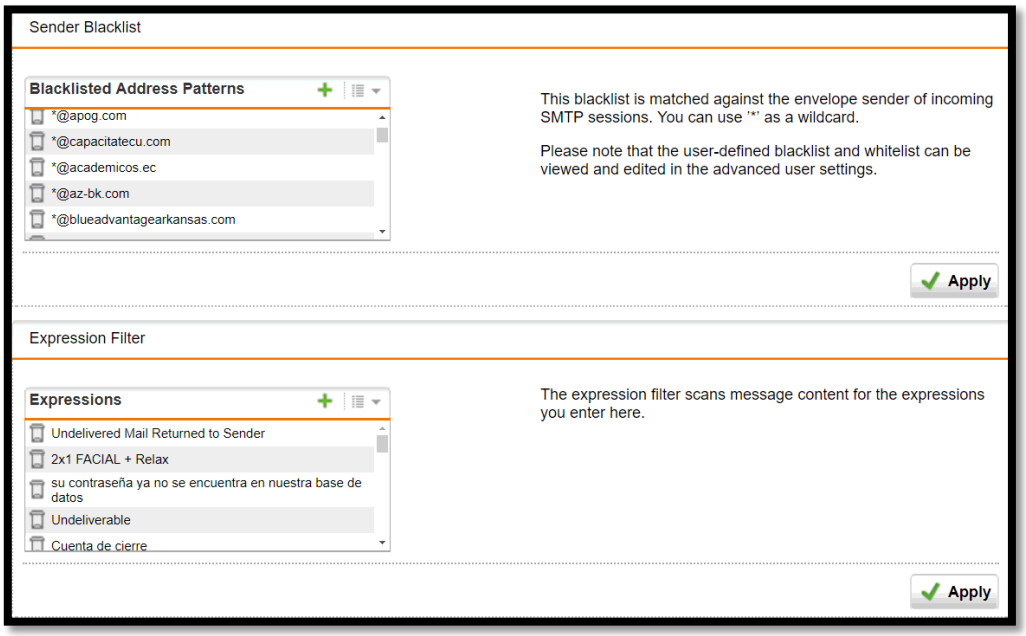


Figura 88. Configurar filtrado de correo por blacklist y expresiones en Sophos.
Elaborado por: Los autores.

- **Webserver Protection**

Se configuró Web Application firewall para la protección del acceso web a los servidores. En lugar de crear un NAT en los puertos 80 o 443, se utiliza este módulo que hace las veces de proxy inverso, para devolver los datos y controlando ataques.

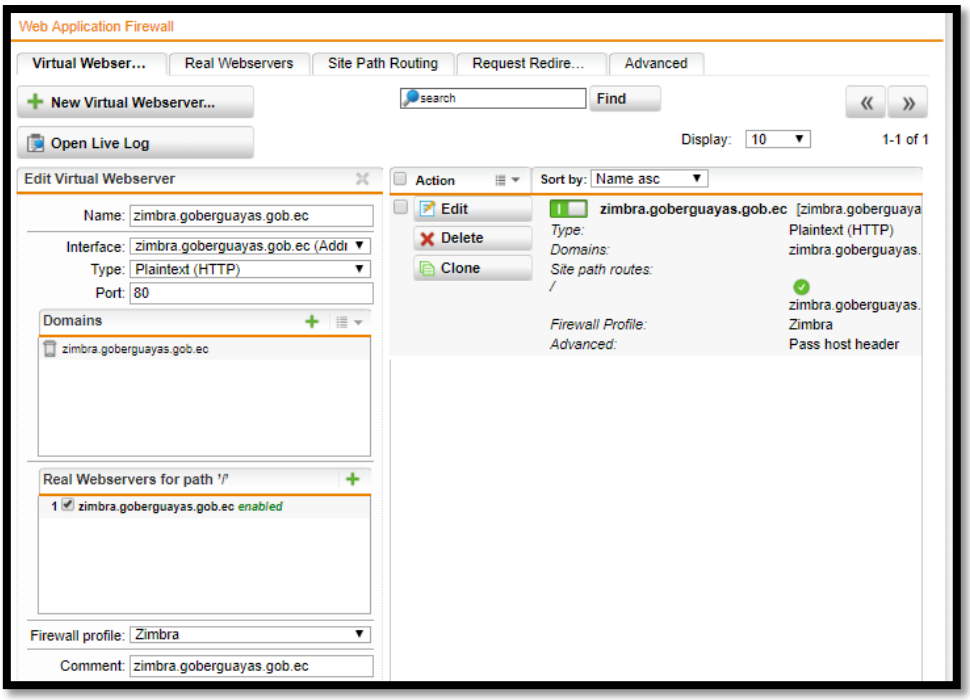


Figura 89. Web Application Firewall en Sophos.
Elaborado por: Los autores.

- **Interfaces & Routing**
  - **Interfaces**

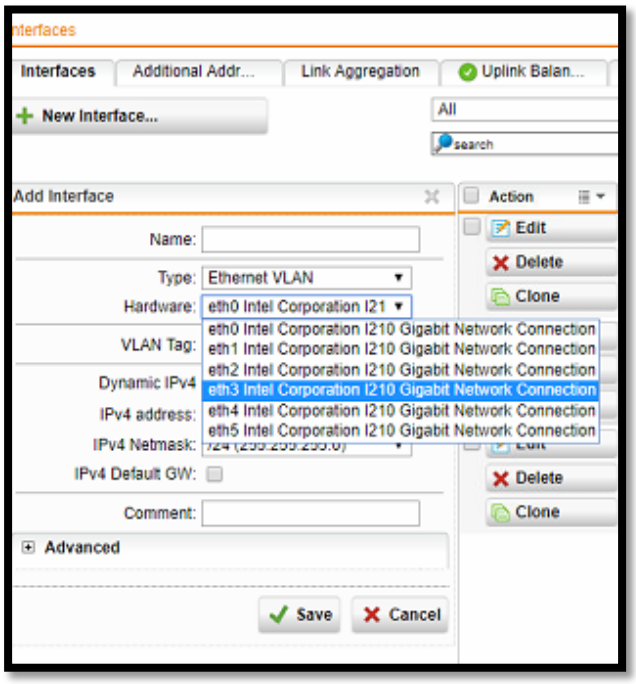


Figura 90 Configuración de interfaz para VLAN
Elaborado por: Los autores.

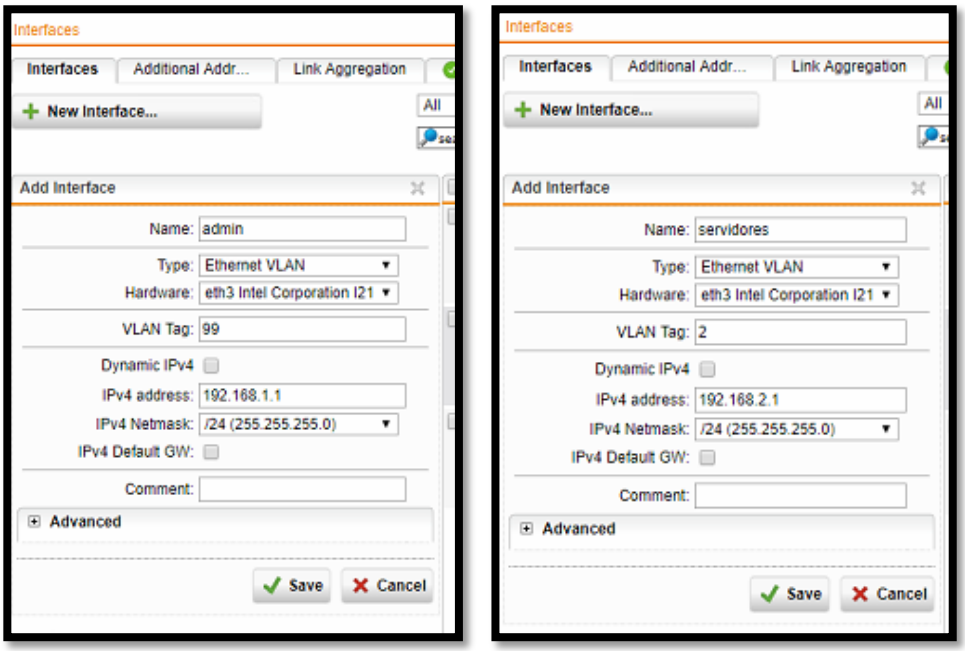


Figura 91 Configuración de VLAN de Administración y servidores
Elaborado por: Los autores.

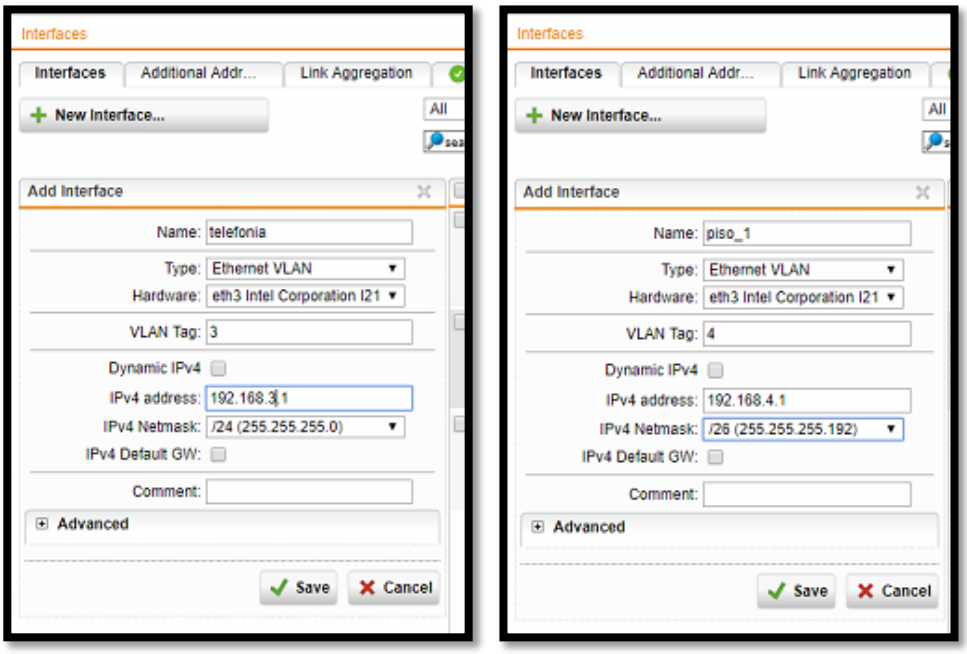


Figura 92 Configuración de VLAN de Telefonía y Piso_!
Elaborado por: Los autores.

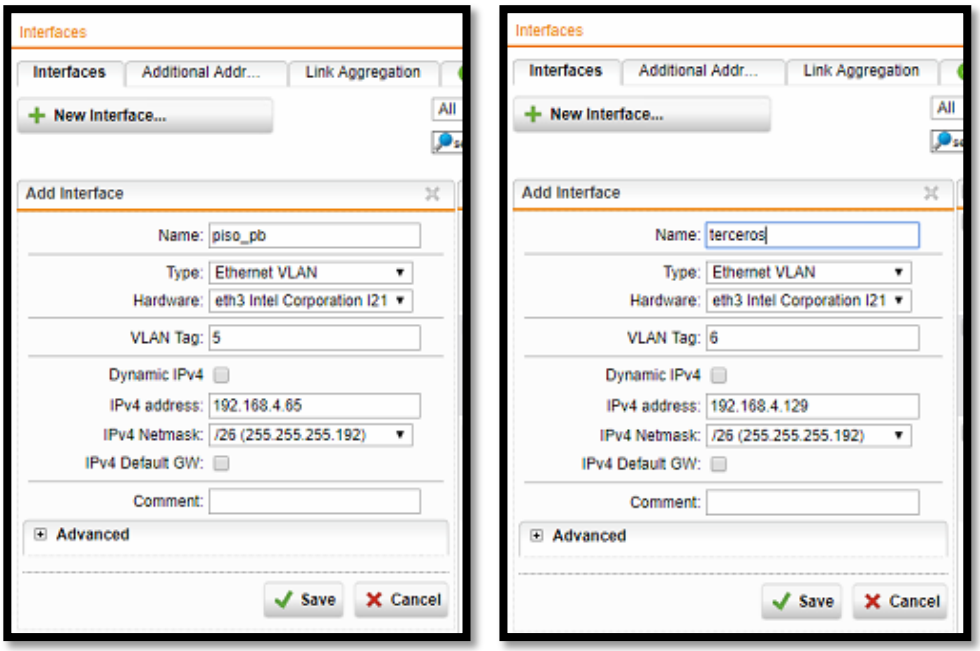


Figura 93 Configuración de VLAN de Piso_PB y Terceros
Elaborado por: Los autores.

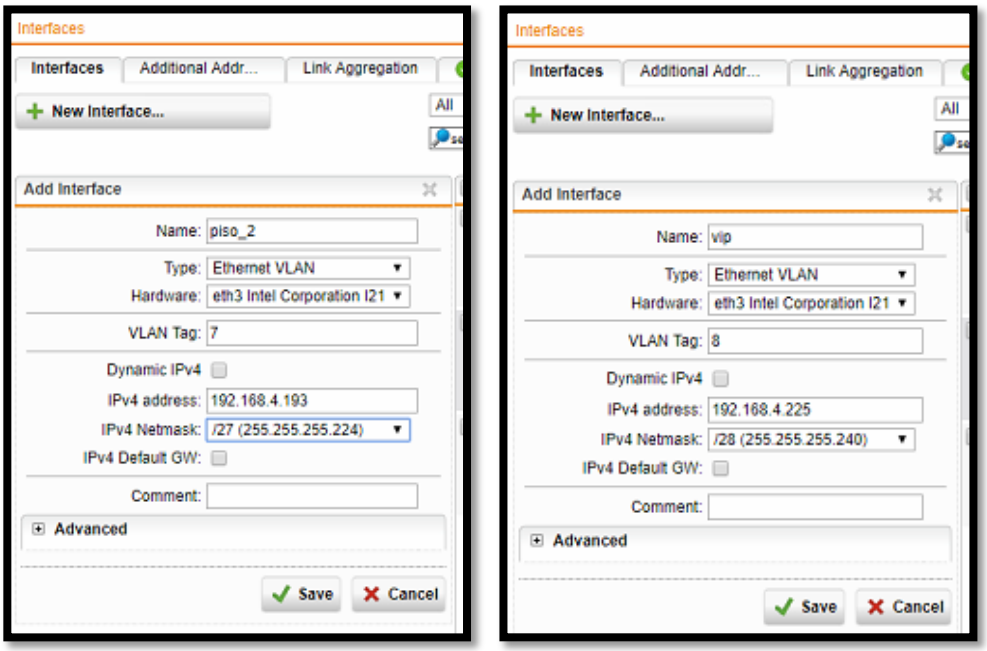


Figura 94 Configuración de VLAN de Piso_2 y VIP
Elaborado por: Los autores.

5.4.5. Identificación de puntos y aplicación de la norma ANSI/TIA/EIA 606A.

Se comenzó identificando todos los puntos de red en cada piso debido a que se desconocía la ubicación de estos, tanto en el punto final como en el patch panel. Una vez identificados se procedió a crear las etiquetas. Se utilizó dos tipos de etiquetas:

- Para la parte posterior del rack y para los puntos finales
- Para ambos extremos del patch panel.

Adicional a esto se crearon los planos por departamento identificando los respectivos puntos de red, mismos que se encuentran en el **Anexo E.**

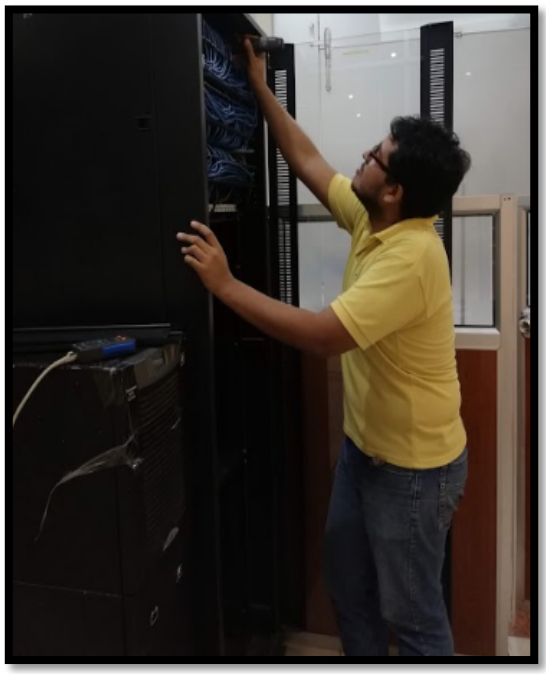


Figura 95. Identificación de puntos en Rack
Elaborado por: Los autores

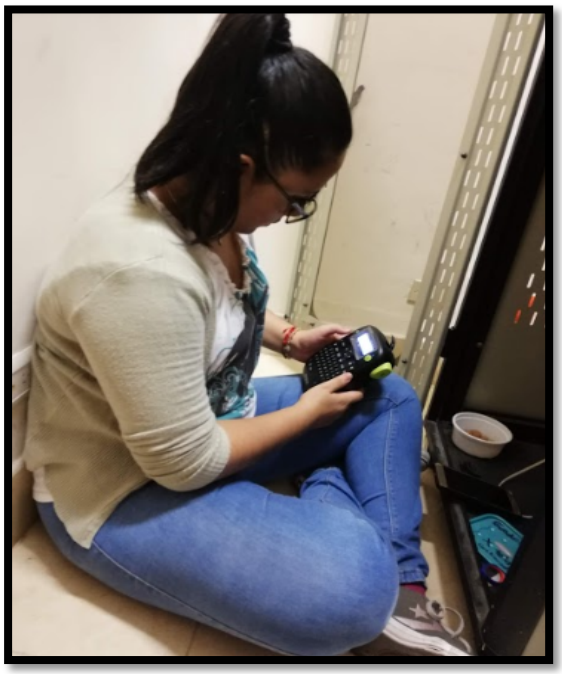


Figura 96. Elaboración de etiquetas
Elaborado por: Los autores

Figura 97. Identificación de puntos finales.
Elaborado por: Los autores

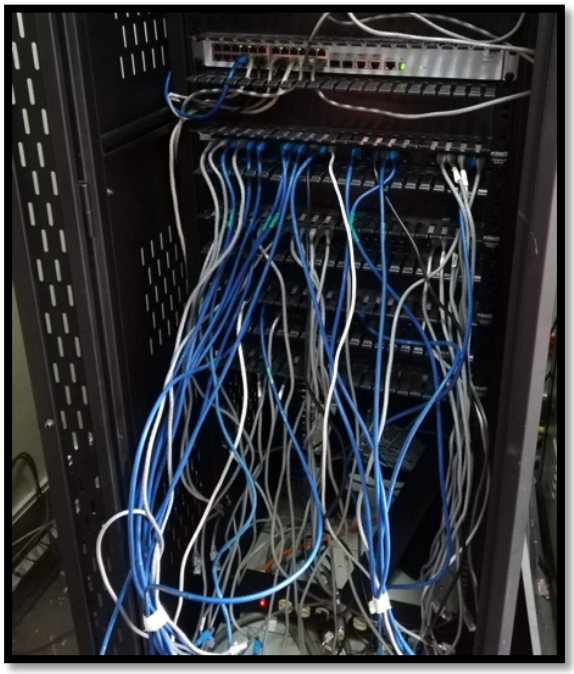


Figura 98. Peinado de patch core.
Elaborado por: Los autores

5.4.6. Elaboración de planos por piso con identificación de etiquetas

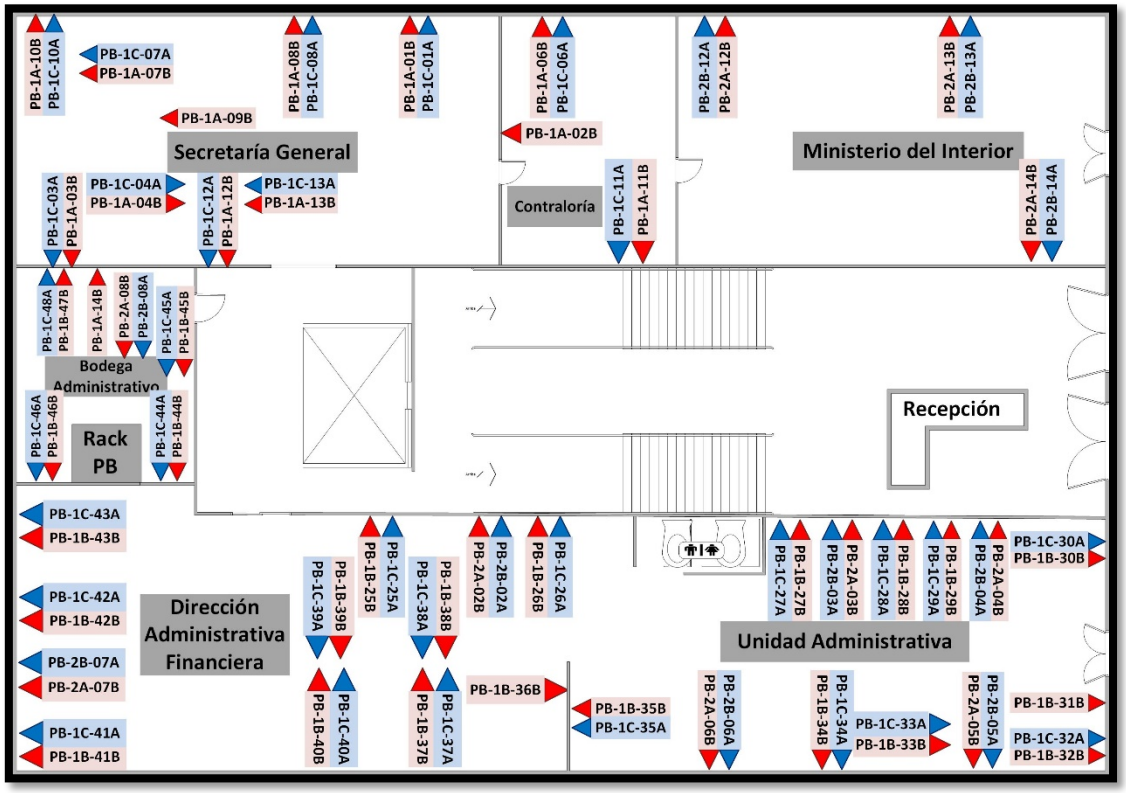


Figura 99 Plano planta baja con etiquetas
Elaborado por: Los autores

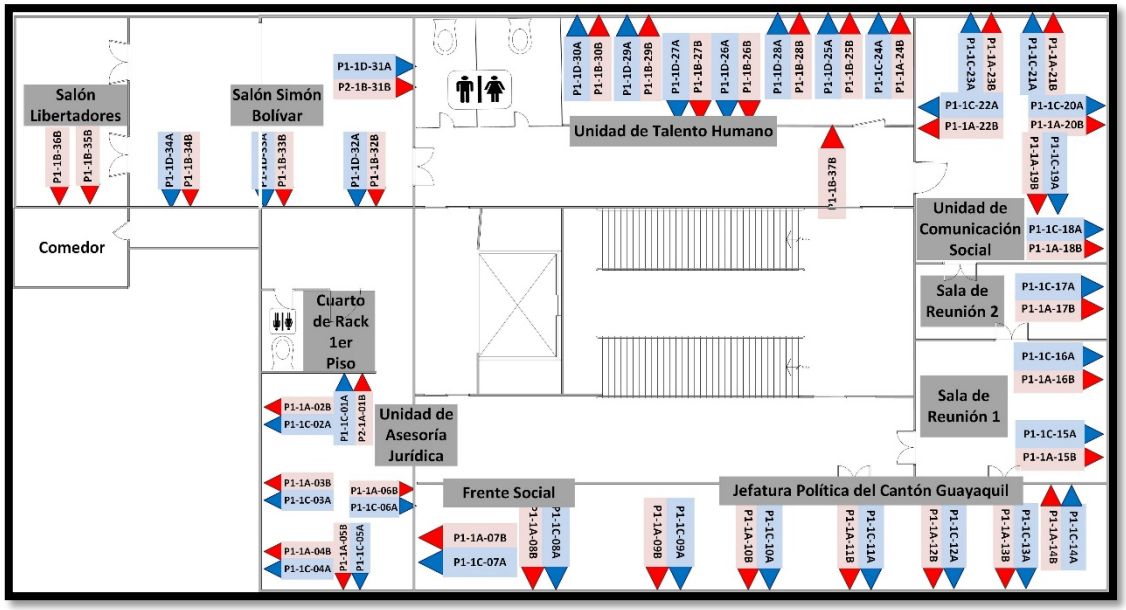


Figura 100 Plano primer piso con etiquetas
Elaborado por: Los autores

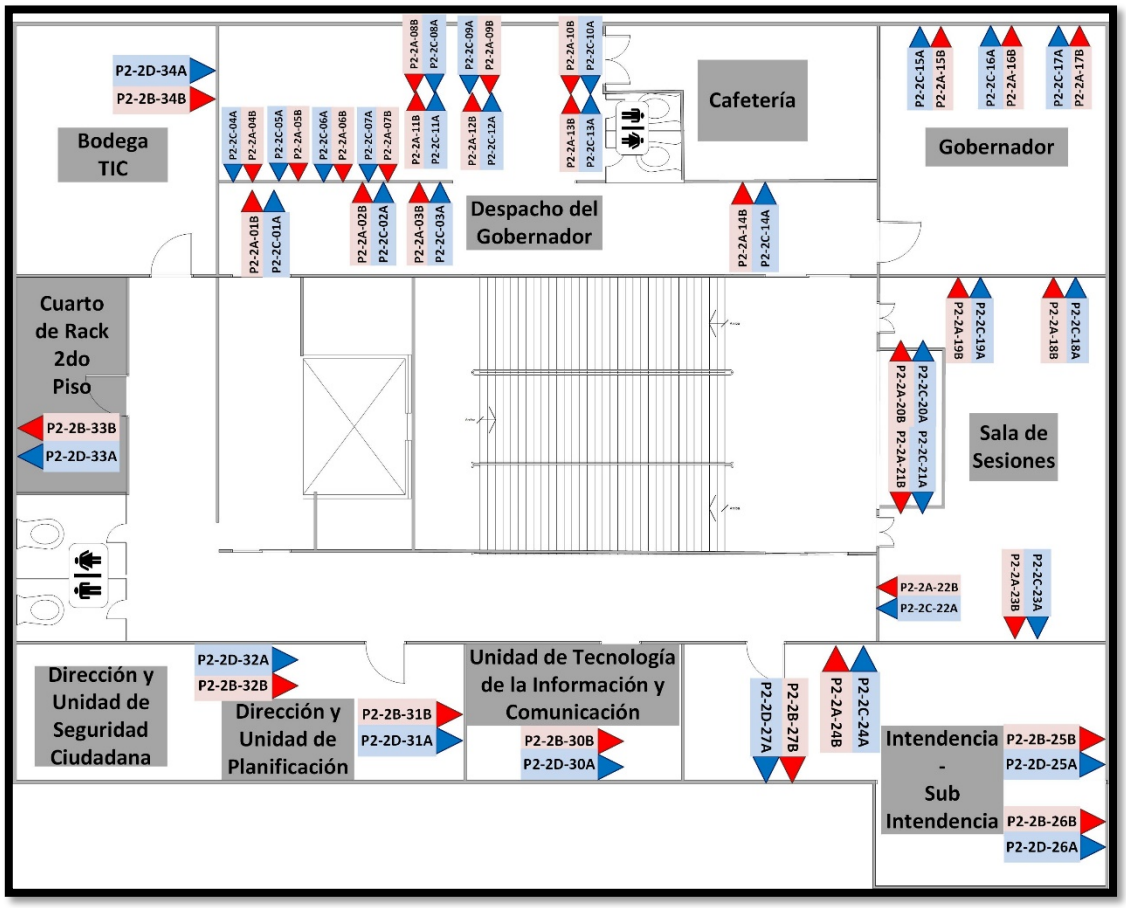


Figura 101 Plano segundo piso con etiquetas
Elaborado por: Los autores

6. Resultados

En la siguiente tabla se detallan los resultados obtenidos en base a los objetivos principales adquiridos para dar soluciones en el presente proyecto:

Tabla 33. Resultados obtenidos por cada objetivo.

Objetivos	Resultados
Reestructurar el direccionamiento IP para establecer un nivel de protección robusto basado en buenas prácticas que abarque tanto a usuarios internos, externos y servidores.	• Mediante la aplicación de VLSM, se obtuvo la máxima eficiencia en el uso del espacio de direccionamiento de la red, puesto que se subdividió la red principal en subredes de acuerdo con la necesidad de cada departamento. • Evitar el desperdicio de direcciones para host. • Aplicación de VLAN para mayor seguridad y control de accesos y permisos de usuarios. • Facilitar la labor del personal de Tecnología con el fin de no llevar un reporte manual de las direcciones Ip ocupadas y disponibles.
Identificar las vulnerabilidades de la red interna para mitigar el impacto de los ataques.	• Con el uso de la herramienta NESSUS se procedió a identificar las vulnerabilidades y debilidades existentes en la red. • Propuesta de adquisición y posterior instalación y configuración del sophos, con el fin de mitigar y corregir las amenazas encontradas; las mismas que afectan a la seguridad de la información

	manipulada en la institución y equipos en general. • Cambio de pertenencia de los equipos de computación de Grupo de trabajo "Workgroup" a dominio "GoberGuayas". • Implementación de políticas de dominio para los equipos de la institución.
Aplicar normas ANSI/TIA/EIA para la administración de cableados y puertos asignados a usuarios en dispositivos capa 2, para garantizar la conectividad de red entre usuarios de la red.	• Organización e identificación de los puntos de red y cableado en los racks existentes en el edificio de planta central. • Etiquetado en cada terminal para mejor identificación del punto. • Planos de la distribución física de puntos de red en todo el edificio de la Gobernación. • Óptima administración de infraestructura de telecomunicaciones.

Elaborado por: Los autores.

6.1. Resultados basados en Active Directory

En este apartado se mostrará la evidencia del funcionamiento de Active Directory en sus diferentes ámbitos.

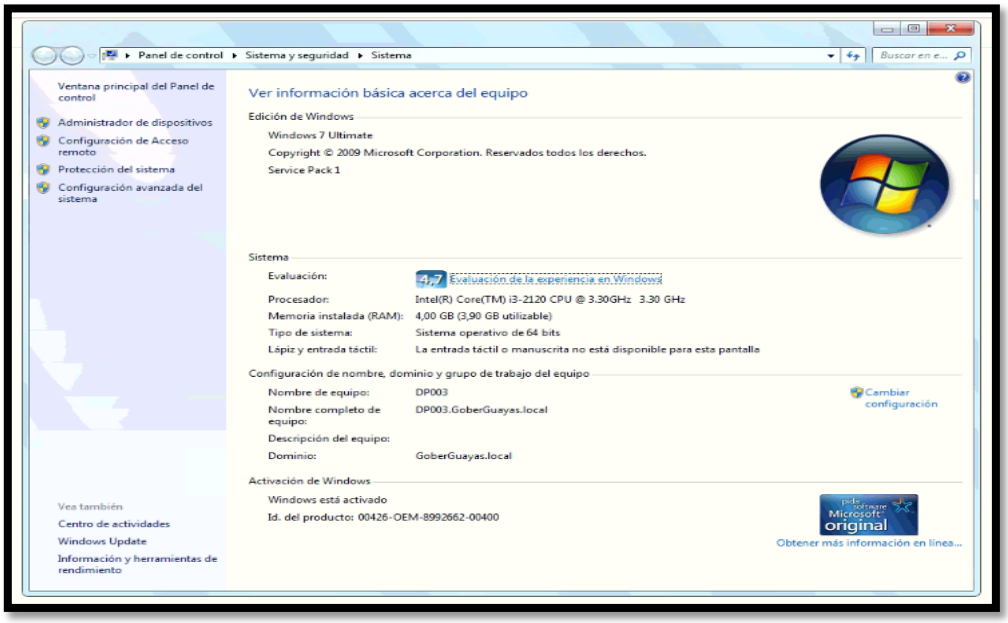


Figura 102. Equipo de usuario en dominio.
Elaborado por: Los autores.

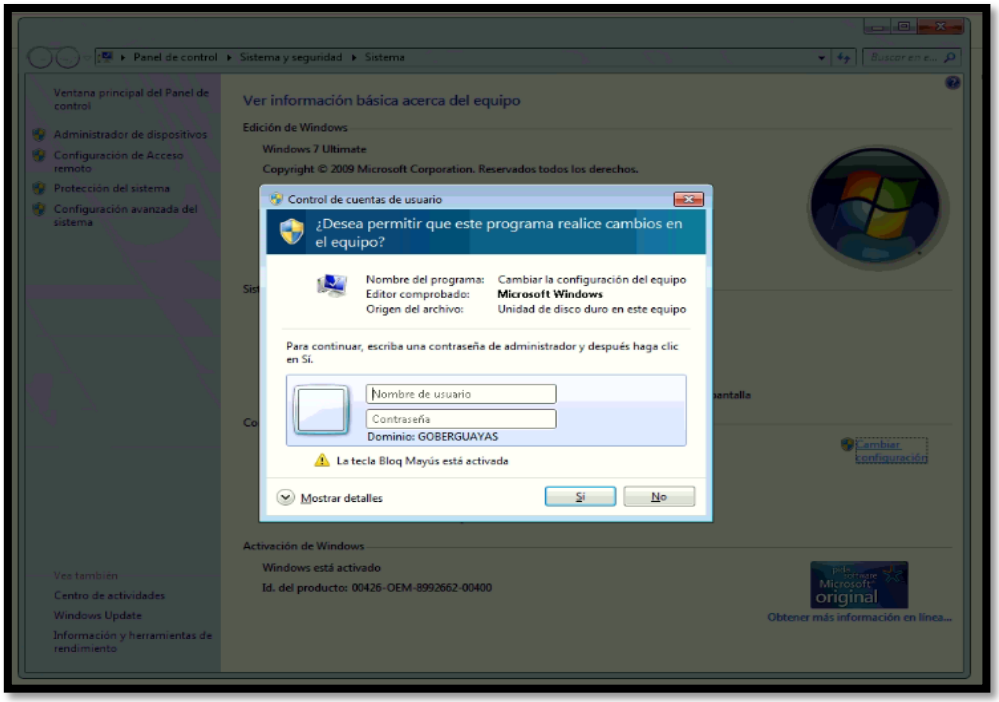


Figura 103. Solicitud de credenciales de administrador para realizar cambios en el equipo.
Elaborado por: Los autores.

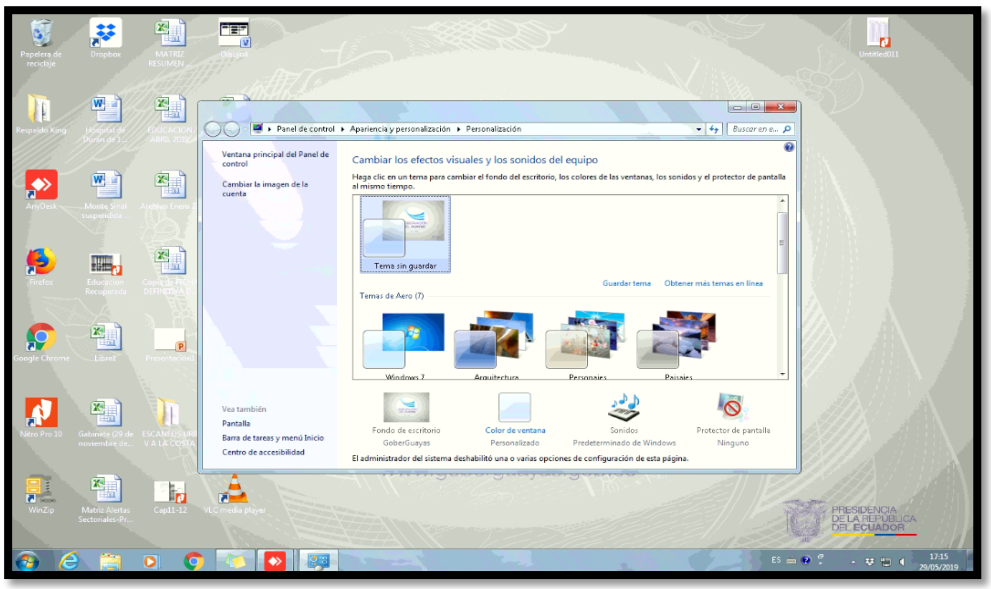


Figura 104. Visualización de política que no permite cambiar el fondo de pantalla.
Elaborado por: Los autores.

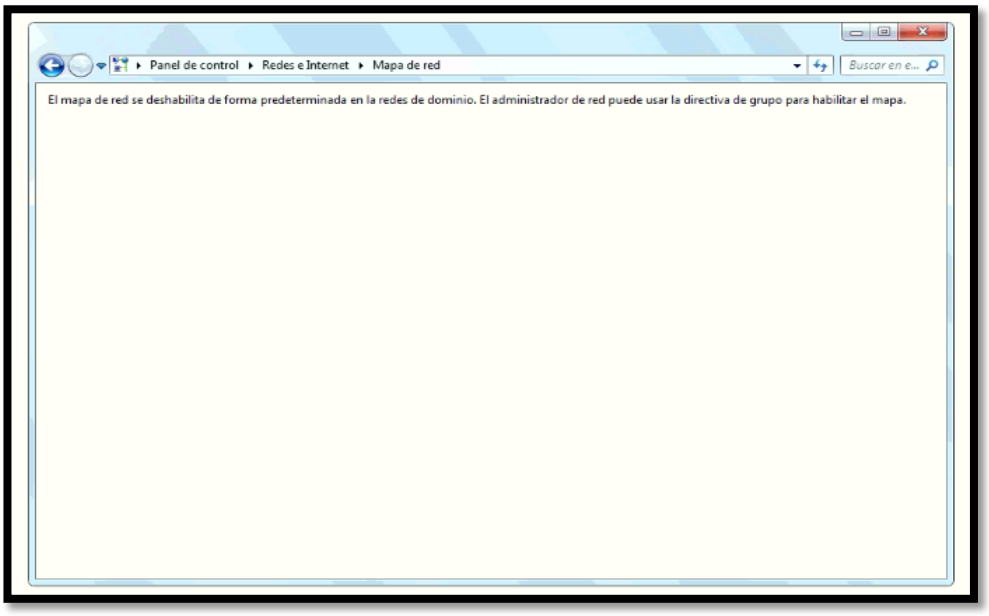


Figura 105. Política que no permite hacer cambios en la configuración de red.
Elaborado por: Los autores.

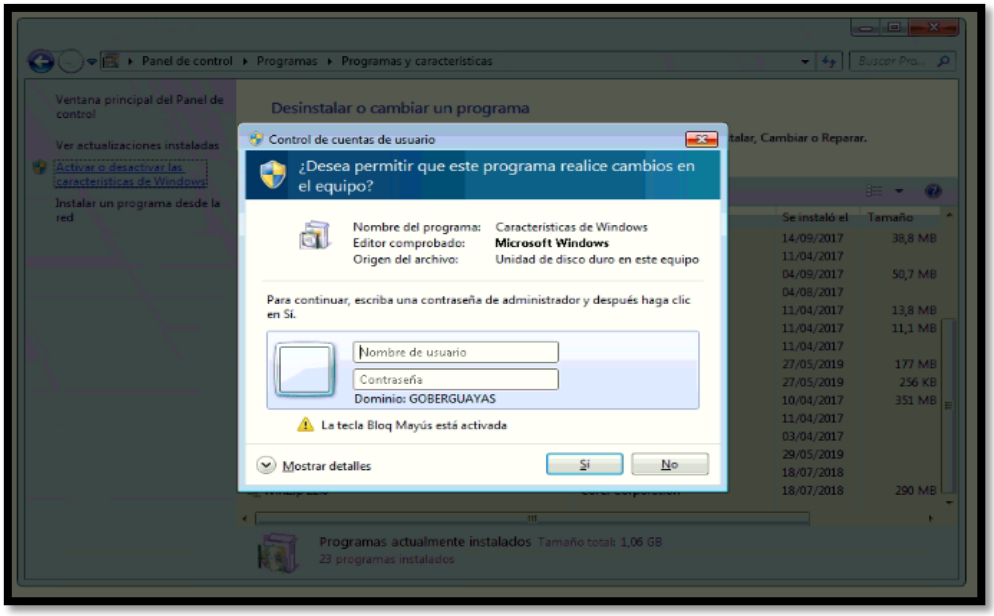


Figura 106. Política para instalación y desinstalación de programas
Elaborado por: Los autores.

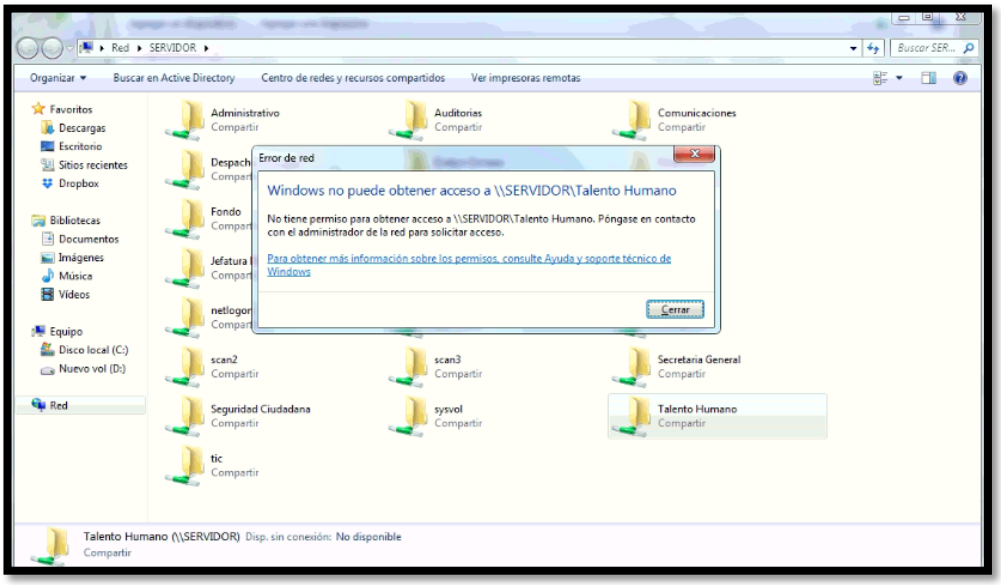


Figura 107. Restricción de acceso a carpeta compartida de otro departamento.
Elaborado por: Los autores.

6.2. Resultados basados en Sophos

En este apartado se mostrará la evidencia del funcionamiento de Sophos en sus diferentes ámbitos.

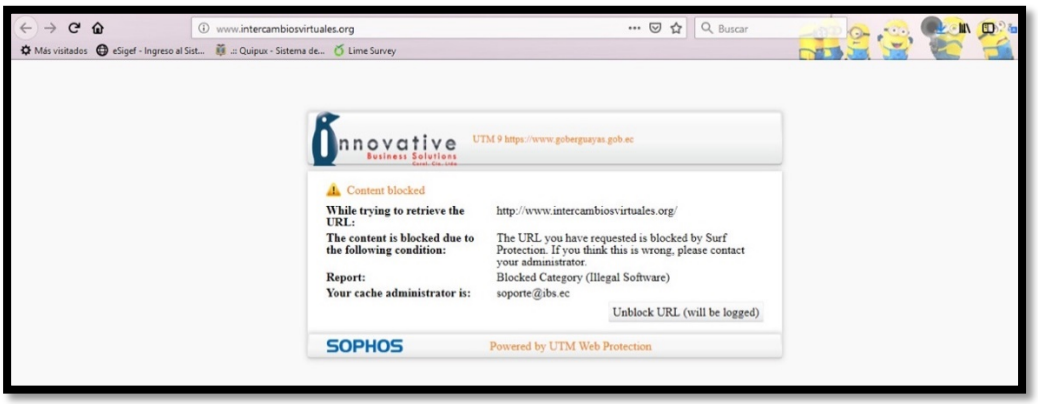


Figura 108. Restricciones de navegación a usuarios.
Elaborado por: Los autores.

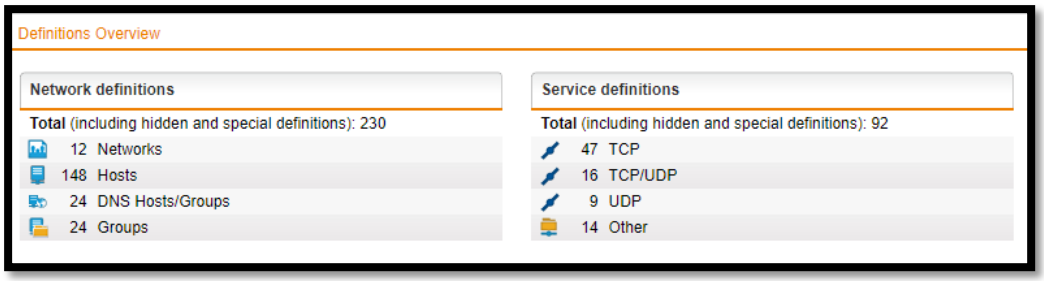


Figura 109. Definiciones de red, usuarios, grupos y servicios.
Elaborado por: Los autores.

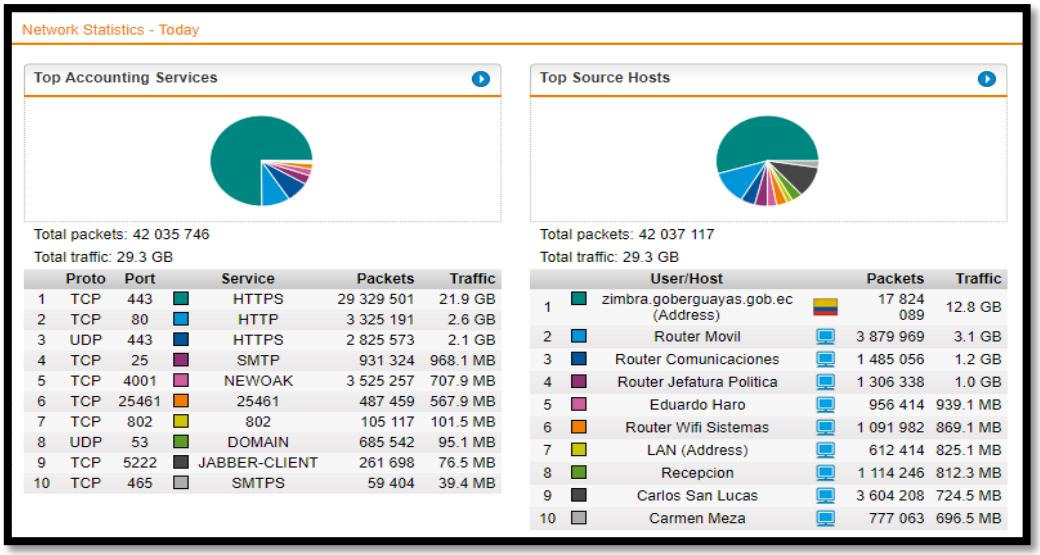


Figura 110. Top de Servicios y Hosts que generan mayor tráfico en la red.
Elaborado por: Los autores.

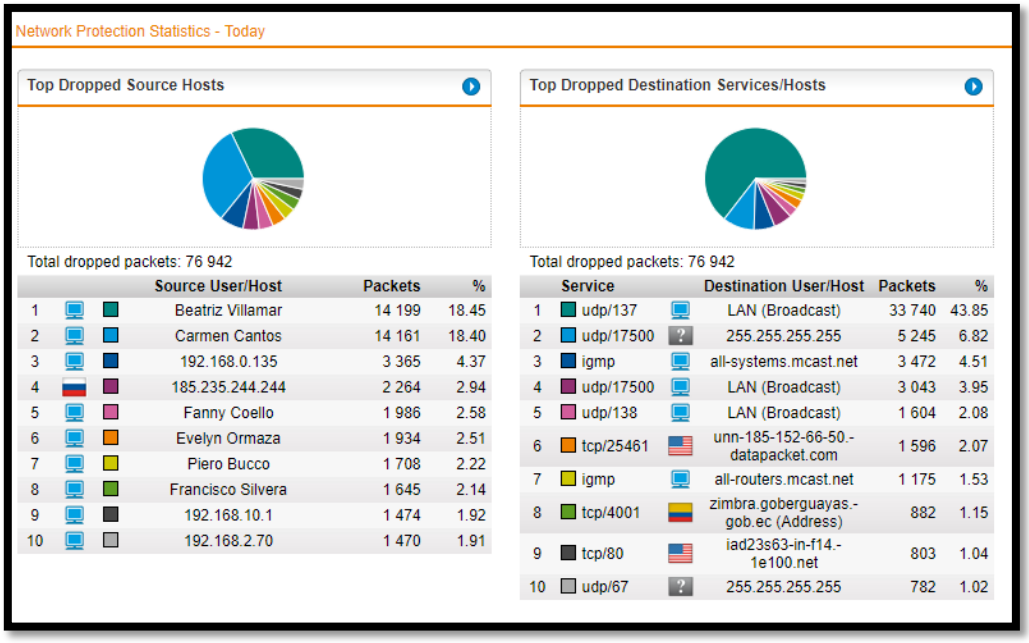


Figura 111. Top de paquetes perdidos por host y por servicio.
Elaborado por: Los autores.

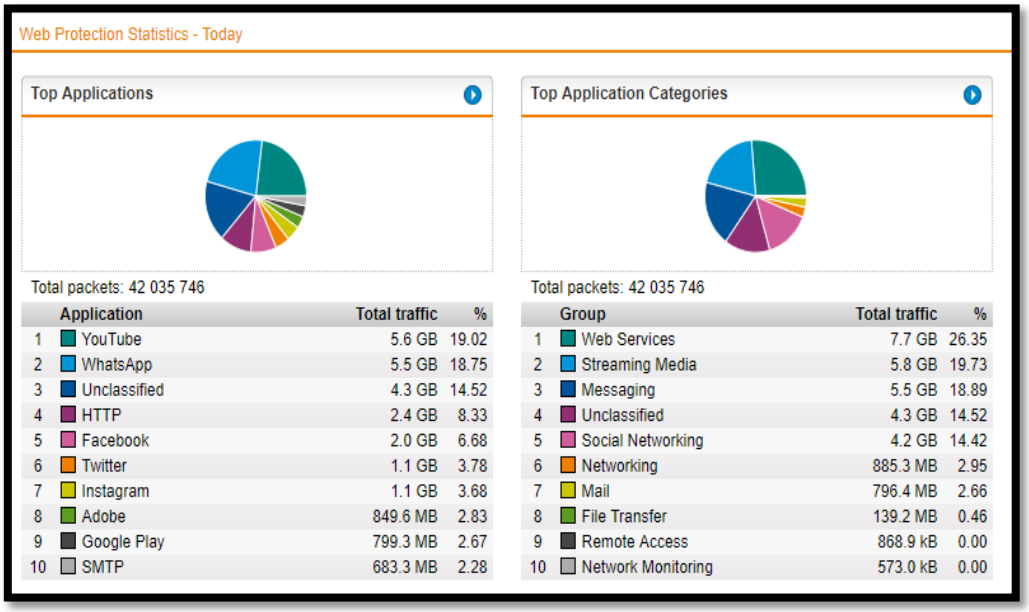
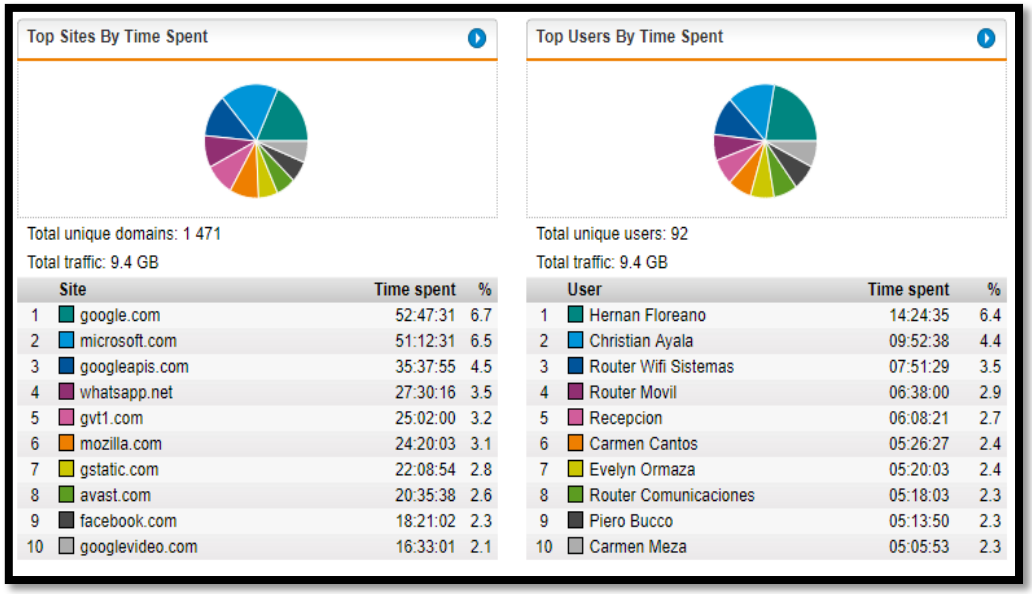


Figura 112. Top de aplicaciones y categorías de aplicaciones que crean mayor tráfico.
Elaborado por: Los autores.



Top Sites By Time Spent

Total unique domains: 1 471

Total traffic: 9.4 GB

	Site	Time spent	%
1	google.com	52:47:31	6.7
2	microsoft.com	51:12:31	6.5
3	googleapis.com	35:37:55	4.5
4	whatsapp.net	27:30:16	3.5
5	gvt1.com	25:02:00	3.2
6	mozilla.com	24:20:03	3.1
7	gstatic.com	22:08:54	2.8
8	avast.com	20:35:38	2.6
9	facebook.com	18:21:02	2.3
10	googlevideo.com	16:33:01	2.1

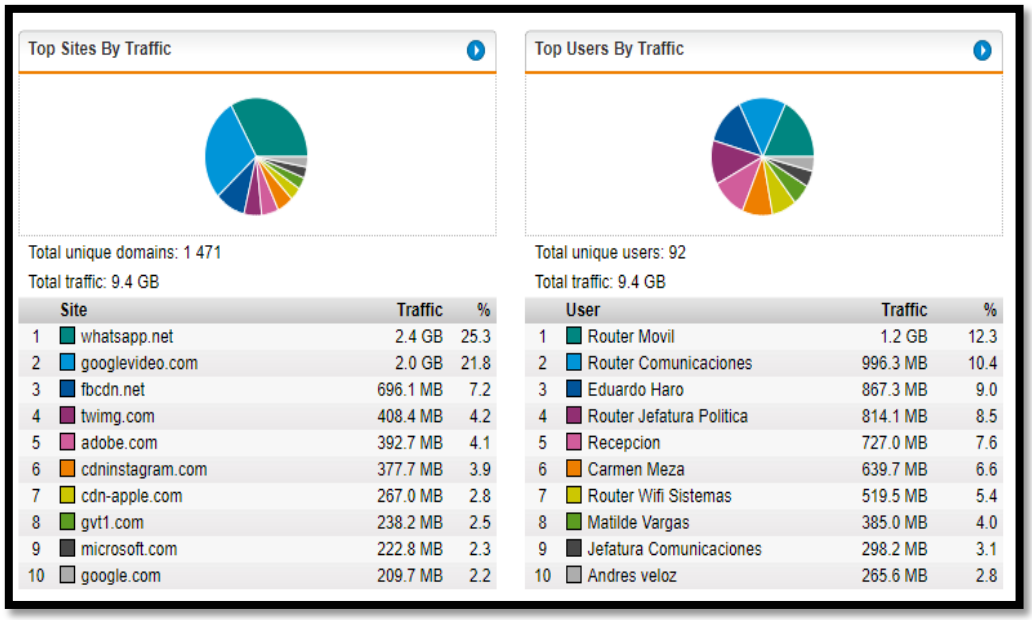
Top Users By Time Spent

Total unique users: 92

Total traffic: 9.4 GB

	User	Time spent	%
1	Hernan Floreano	14:24:35	6.4
2	Christian Ayala	09:52:38	4.4
3	Router Wifi Sistemas	07:51:29	3.5
4	Router Movil	06:38:00	2.9
5	Recepcion	06:08:21	2.7
6	Carmen Cantos	05:26:27	2.4
7	Evelyn Ormaza	05:20:03	2.4
8	Router Comunicaciones	05:18:03	2.3
9	Piero Bucco	05:13:50	2.3
10	Carmen Meza	05:05:53	2.3

Figura 113. Top de tiempo de navegación por sitio y usuarios.
Elaborado por: Los autores.



Top Sites By Traffic

Total unique domains: 1 471

Total traffic: 9.4 GB

	Site	Traffic	%
1	whatsapp.net	2.4 GB	25.3
2	googlevideo.com	2.0 GB	21.8
3	fbcdn.net	696.1 MB	7.2
4	twimg.com	408.4 MB	4.2
5	adobe.com	392.7 MB	4.1
6	cdninstagram.com	377.7 MB	3.9
7	cdn-apple.com	267.0 MB	2.8
8	gvt1.com	238.2 MB	2.5
9	microsoft.com	222.8 MB	2.3
10	google.com	209.7 MB	2.2

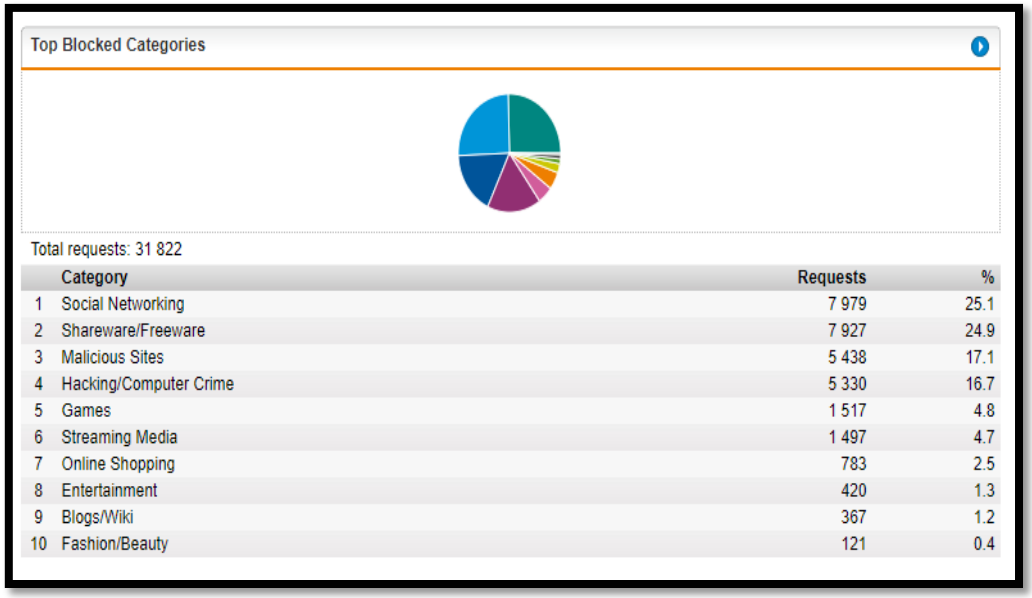
Top Users By Traffic

Total unique users: 92

Total traffic: 9.4 GB

	User	Traffic	%
1	Router Movil	1.2 GB	12.3
2	Router Comunicaciones	996.3 MB	10.4
3	Eduardo Haro	867.3 MB	9.0
4	Router Jefatura Politica	814.1 MB	8.5
5	Recepcion	727.0 MB	7.6
6	Carmen Meza	639.7 MB	6.6
7	Router Wifi Sistemas	519.5 MB	5.4
8	Matilde Vargas	385.0 MB	4.0
9	Jefatura Comunicaciones	298.2 MB	3.1
10	Andres veloz	265.6 MB	2.8

Figura 114. Top de sitios y usuarios que generan mayor tráfico.
Elaborado por: Los autores.

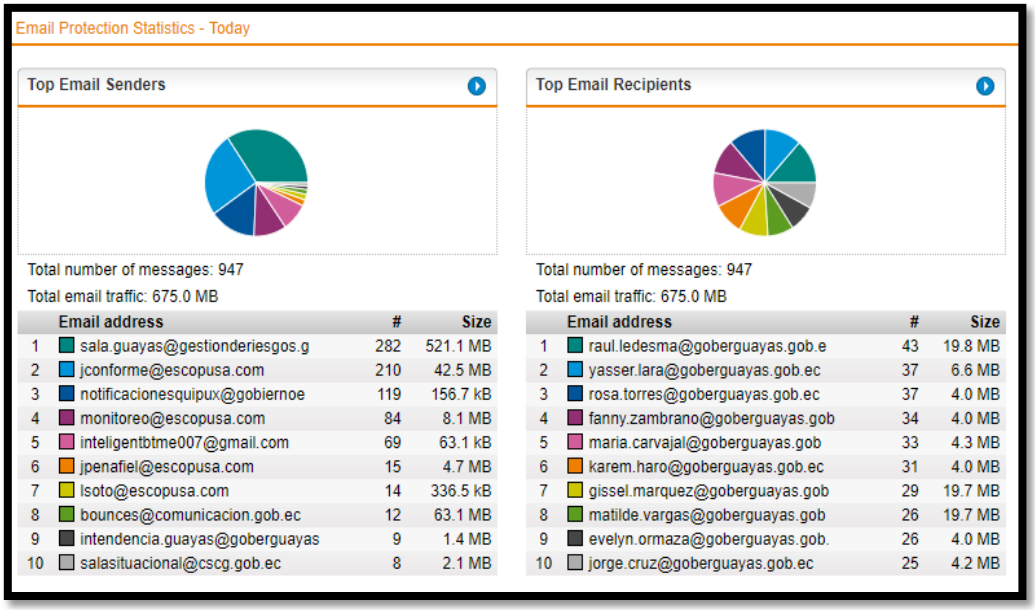


Top Blocked Categories

Total requests: 31 822

	Category	Requests	%
1	Social Networking	7 979	25.1
2	Shareware/Freeware	7 927	24.9
3	Malicious Sites	5 438	17.1
4	Hacking/Computer Crime	5 330	16.7
5	Games	1 517	4.8
6	Streaming Media	1 497	4.7
7	Online Shopping	783	2.5
8	Entertainment	420	1.3
9	Blogs/Wiki	367	1.2
10	Fashion/Beauty	121	0.4

Figura 115. Top de categorías bloqueadas.
Elaborado por: Los autores.



Email Protection Statistics - Today

Top Email Senders

Total number of messages: 947

Total email traffic: 675.0 MB

	Email address	#	Size
1	sala.guayas@gestionderiesgos.g	282	521.1 MB
2	jconforme@escopusa.com	210	42.5 MB
3	notificacionesquipux@gobiernoe	119	156.7 kB
4	monitoreo@escopusa.com	84	8.1 MB
5	inteligentbtme007@gmail.com	69	63.1 kB
6	jpenafiel@escopusa.com	15	4.7 MB
7	lsoto@escopusa.com	14	336.5 kB
8	bounces@comunicacion.gob.ec	12	63.1 MB
9	intendencia.guayas@goberguayas	9	1.4 MB
10	salasituacional@cscg.gob.ec	8	2.1 MB

Top Email Recipients

Total number of messages: 947

Total email traffic: 675.0 MB

	Email address	#	Size
1	raul.ledesma@goberguayas.gob.e	43	19.8 MB
2	yasser.lara@goberguayas.gob.ec	37	6.6 MB
3	rosa.torres@goberguayas.gob.ec	37	4.0 MB
4	fanny.zambrano@goberguayas.gob	34	4.0 MB
5	maria.carvajal@goberguayas.gob	33	4.3 MB
6	karem.haro@goberguayas.gob.ec	31	4.0 MB
7	gissel.marquez@goberguayas.gob	29	19.7 MB
8	matilde.vargas@goberguayas.gob	26	19.7 MB
9	evelyn.ormaza@goberguayas.gob.	26	4.0 MB
10	jorge.cruz@goberguayas.gob.ec	25	4.2 MB

Figura 116. Top de envío y recepción de correo por usuarios
Elaborado por: Los autores.

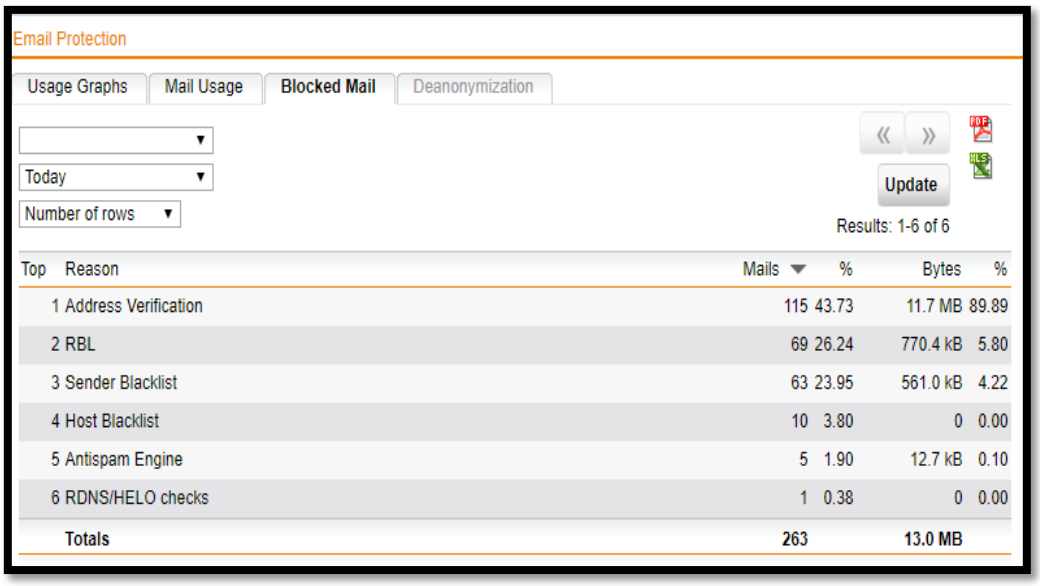


Figura 117. Listado de razones por las que se bloquea correos.
Elaborado por: Los autores.

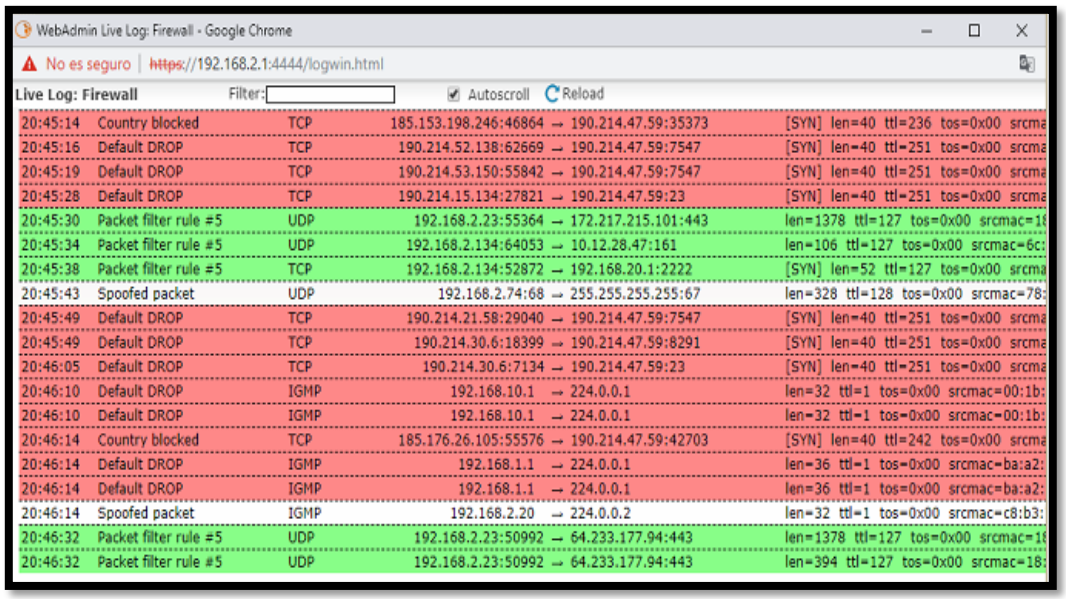


Figura 118 Validación de tráfico a través del firewall
Elaborado por: Los autores.

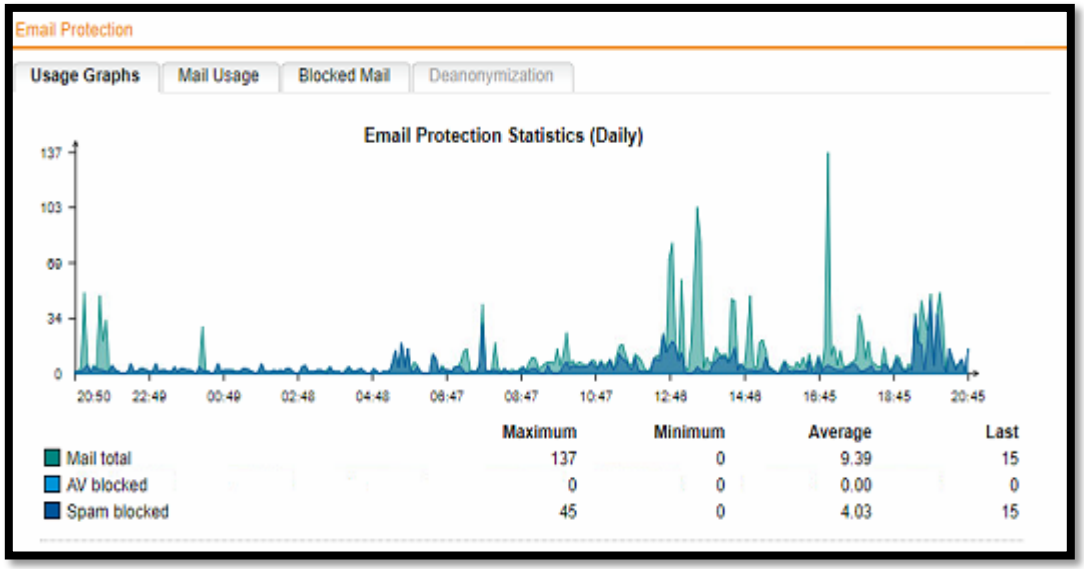


Figura 119 Gráfico estadístico de la Protección de Correo
Elaborado por: Los autores.

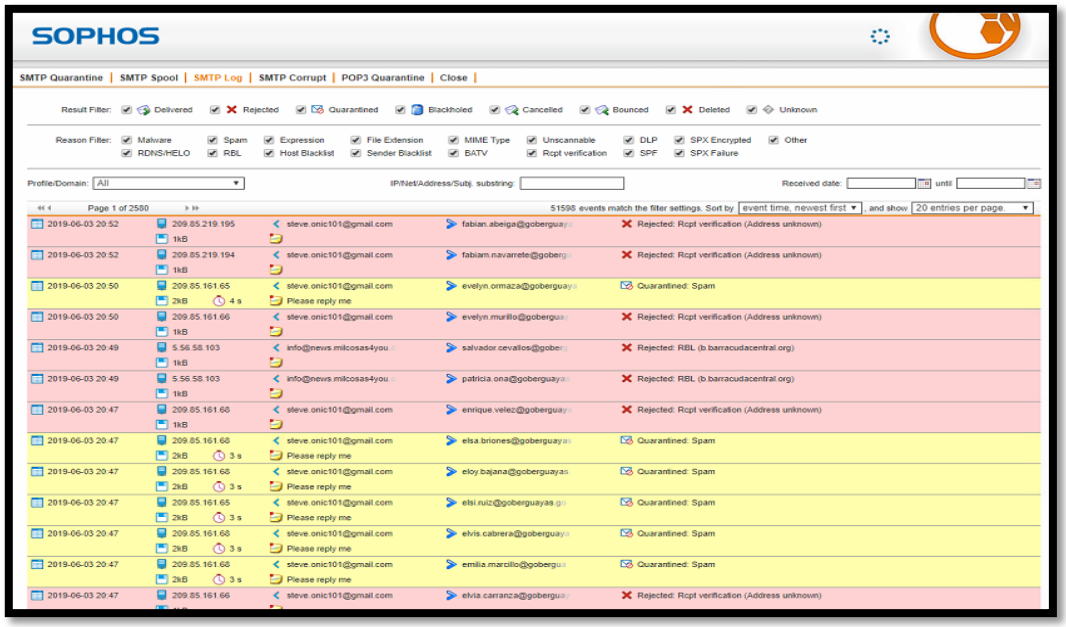


Figura 120 Reporte de Correo bloqueado y en cuarentena
Elaborado por: Los autores.

6.3. Resultados basados en Norma ANSI/TIA/EIA 606A

En este apartado se mostrará todos los resultados obtenidos al realizar las diferentes fases sobre el etiquetado del cableado estructurado.

Figura 121. Etiquetado de Patch Core en el Rack 1 del Piso 2.
Elaborado por: Los autores

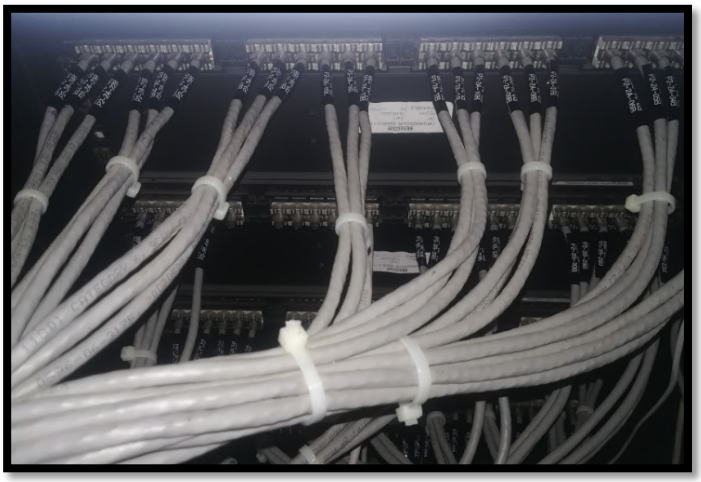


Figura 122. Etiquetado del cable en el Patch Panel del Rack 1 en el Piso 2.
Elaborado por: Los autores

Figura 123. Etiquetado de los Patch Core en el Rack 1 del Piso 1.
Elaborado por: Los autores

Figura 124. Etiquetas en Patch Core.
Elaborado por: Los autores

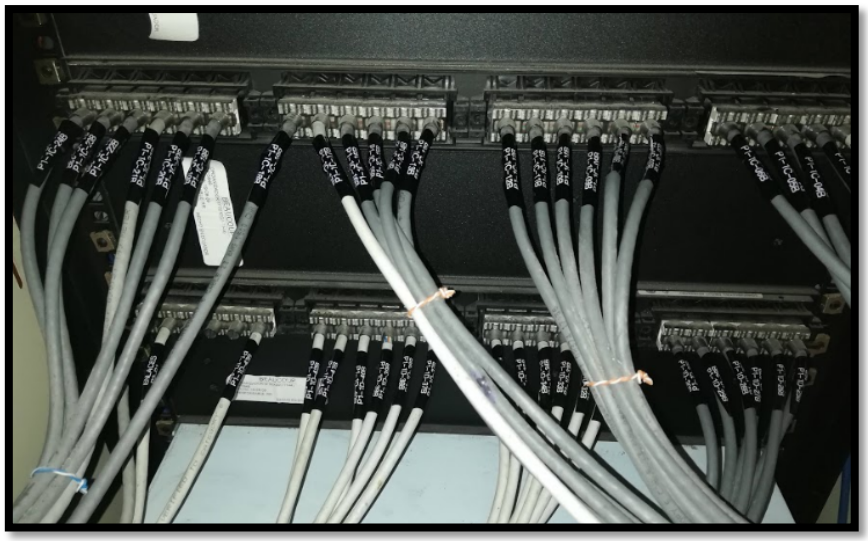


Figura 125. Etiquetado del cable en el Patch Panel del Rack 1 en el Piso 1.
Elaborado por: Los autores

Figura 126. Etiquetado del Patch Panel en el Rack 1 de Planta baja.
Elaborado por: Los autores

Figura 127. Etiquetado del cable en el Patch Panel del Rack 1 de Planta baja.
Elaborado por: Los autores

Figura 128. Etiquetado de Patch Core del Rack 2 de Planta baja.
Elaborado por: Los autores

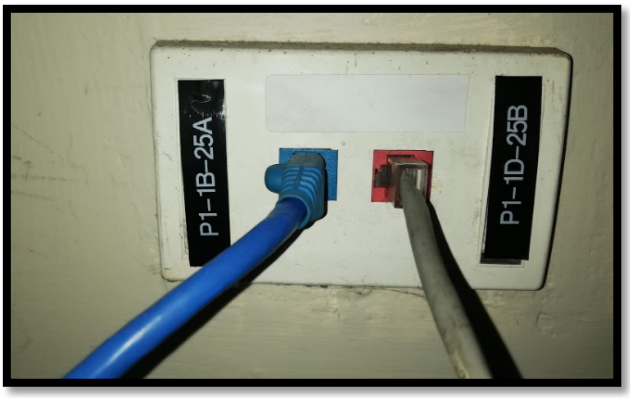


Figura 129. Etiquetado de punto de usuario.
Elaborado por: Los autores

7. Conclusiones

La reestructuración del direccionamiento IP mediante buenas prácticas como son VLSM e implementación de VLAN, servirá para que la Gobernación del Guayas administre eficientemente la red, evitando desperdiciar espacio de direccionamiento y brindará un nivel más robusto de seguridad a sus usuarios.

La implementación del Directorio Activo como medida de seguridad permitirá disminuir el costo y esfuerzo de la administración de la red del dominio GoberGuayas, lo cual facilitará la centralización de los recursos y de gestión, así como la autenticación y autorización de usuarios.

El diseño e implementación de un esquema de seguridad perimetral mediante el firewall UTM y el servidor de domino, permite que la Unidad de Tecnologías de la información y comunicación pueda mitigar el impacto de las vulnerabilidades encontradas, a su vez, controlar el tráfico, restringir accesos a usuario, protección de correo, entre otras características que beneficiarán la experiencia de navegación del usuario.

La aplicación de las normas de etiquetado ANSI/TIA/EIA permitirá a la Gobernación del Guayas tener la capacidad de escalabilidad en la red, así como brindar el máximo rendimiento de la Unidad de Tecnologías de la Información y Comunicación, al disponer de una administración y gestión, rápida y sencilla.

8. Recomendaciones

Renovación y reorganización de los switches ya que no brindan una administración eficiente por si solos y necesitan complementarse con otros equipos, se debe reorganizar la interconexión entre switches para evitar pérdidas en el recorrido de los paquetes.

Mantener actualizado el Sistema Operativo del Servidor de Directorio Activo con el fin de amenorar la vulnerabilidad de posibles ataques.

Mantener una constante revisión de los reportes que se pueden obtener en el dispositivo UTM y llevar un control de usuarios acorde a las normas establecidas por la Gobernación del Guayas.

Planificar correctamente el crecimiento o reestructuración de ciertos departamentos que demandarán más usuarios de la red, para la correcta administración de esta y evitar el uso de equipos caseros que no brindan ninguna seguridad.

9. Referencias bibliográficas

Tanebaum | Wetherall. (2012). *Redes de computadoras.* México: Pearson.

López, A. A. (2005). *La red Internet. El modelo TCP/IP.* Grupo Abantos Formación y Consultoría.

Andreu, J. (2014). *Redes locales.* México: Editex.

Rabadán, N. (2008). *Guiaimpresón.* Obtenido de http://guiaimpresion.com.ar/lib/noticias/317.php

Londoño, J. (2014). *Seguridad Informática.* Medellín.

Aguilera, P. (2010). *Seguridad Informática.* México: Editex.

Gascó, G. E., Serrano, R. R., & Ramada, J. D. (2013). *Seguridad informática.* Macmillan Profesional.

Cameron, R., Woodberg, B., Giecco, P., Eberhard, T., & Quinn, J. (2010). *Junos Security.* Sebastopol: O'Reilly Media, Inc.

Molina, J., & Baena, L. (2007). *Sistemas Operativos en Entornos monousuario y multiusuario.* Editorial Visión Libros.

Trejos S., H. F. (2013). *Administración de Dominios Windows Server 2008 R2.* Armenia, Quindío, Colombia: Universidad del Quindío.

BRADY. (2006). ANSI/TIA/EIA/606A Quick Reference Guide. *Administration Standard for Telecommunications Infrastructure*. Milwaukee, Wisconsin, Estados Unidos: BRADY.

Vasco, M. (Octubre de 2010). *Dimensionamiento de una central telefónica IP utilizando estandares abiertos y software libre para la empresa conectividad global.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/2497/1/CD-3199.pdf

Jhuéz, J. (2018). *Metodologías para la gestión de riesgo.* Obtenido de J.Jhuéz International: https://capacitacioncgr.jovenclub.cu/wp-content/uploads/2018/05/Metodologia-para-la-Gestion-del-Riesgo.pdf

Gerónimo, A. F. (2009). *Modelo OSI.* El Cid Editor | apuntes.

Edwards, W. (2005). *CCNP complete study guide.* San Francisco: London Sybex.

10. Anexos

10.1. Anexo A: Entrevista con el responsable del Área de TIC's

Siendo 02 de abril de 2018 aproximadamente a las 08h30, se llevó a cabo una reunión con el Ing. Gabriel Proaño Manosalvas, administrador de la red y Responsable de la Unidad de Tecnología de la Información y Comunicaciones de la Gobernación de la Provincia del Guayas, con el fin de reconocer las problemáticas y el alcance de este proyecto técnico dentro de la institución.

De acuerdo con las siguientes preguntas que se detallan a continuación:

- ¿Cuáles son las funciones que ejecuta el departamento de Sistemas?
- ¿Cuáles son las limitantes encontradas para el correcto cumplimiento de las funciones del departamento de sistemas?
- ¿Quién administra los equipos de red y servicios?
- ¿Posee planos donde se identifiquen los puntos que se encuentran activos en la actualidad?
- ¿Cómo está estructurada la red de Planta Central?
- ¿Qué, cuáles y cuántos dispositivos de red posee la gobernación?
- ¿Cuáles son las herramientas con las que cuentan para la administración de la red?
- ¿Qué servicios provee la institución?
- ¿Cuáles son las políticas internas a nivel de la red?
- ¿Qué políticas se desea aplicar y el motivo?
- ¿Qué seguridades se le provee a la red de la institución?
- ¿Cuál es el procedimiento de identificación de un punto de red para su habilitación?

10.2. Anexo B: Encuesta a los funcionarios públicos

Con el objetivo de conocer el nivel de satisfacción de los funcionarios públicos que laboran en el edificio de Planta Central de la Gobernación del Guayas con respecto a los servicios de red e internet que usan en la actualidad, se procedió a crear la siguiente encuesta, que consta con las interrogantes que se detallan a continuación:

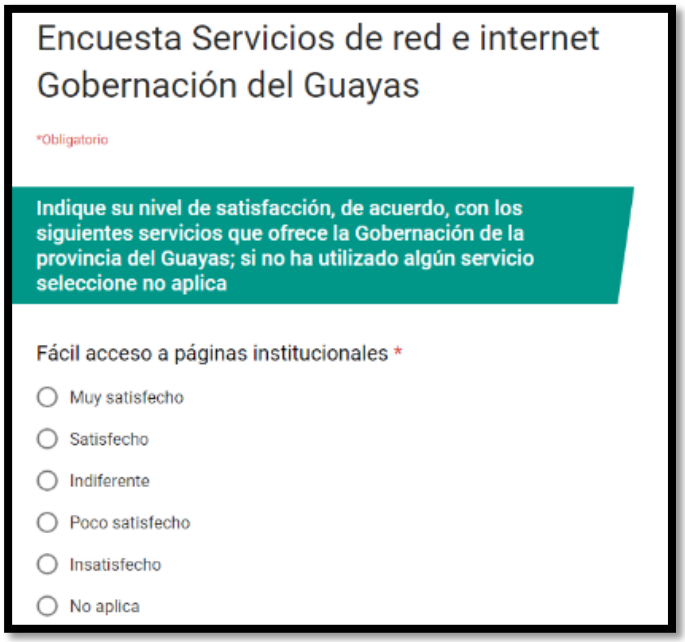


Figura 130 Diseño de encuesta primera parte
Elaborado por: Los autores.

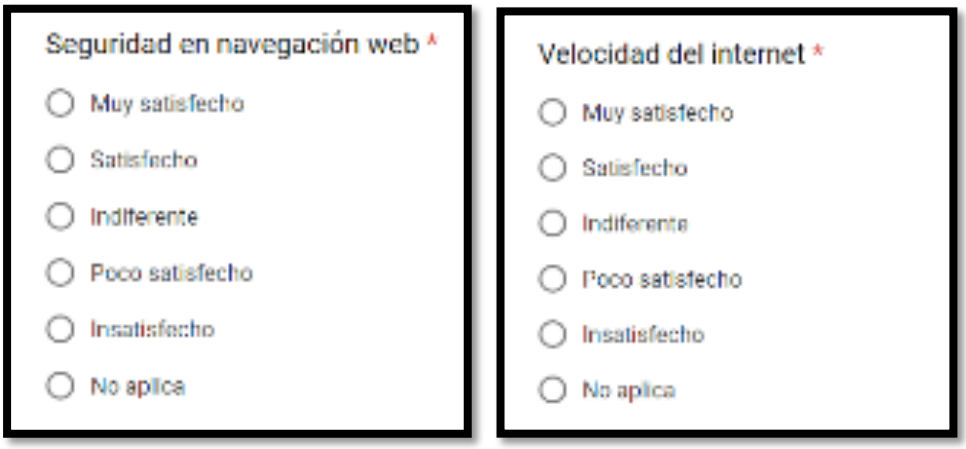


Figura 131 Diseño de encuesta segunda parte
Elaborado por: Los autores.

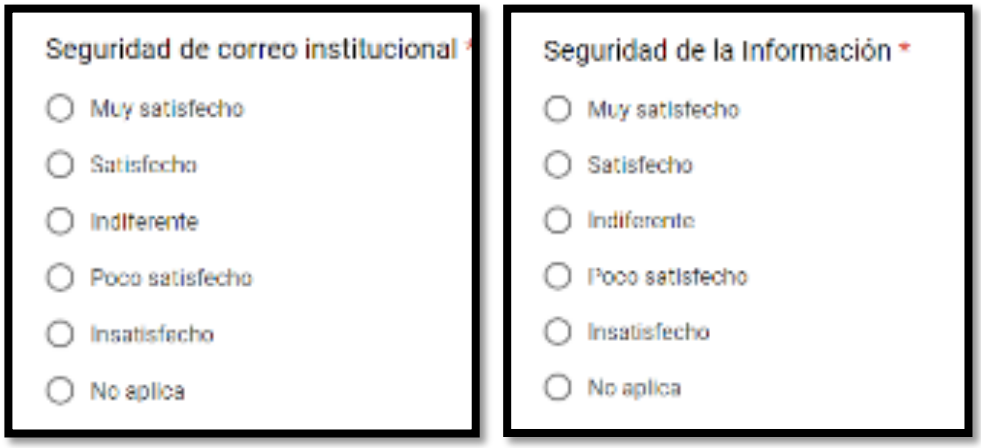


Figura 132 Diseño de encuesta tercera parte
Elaborado por: Los autores.

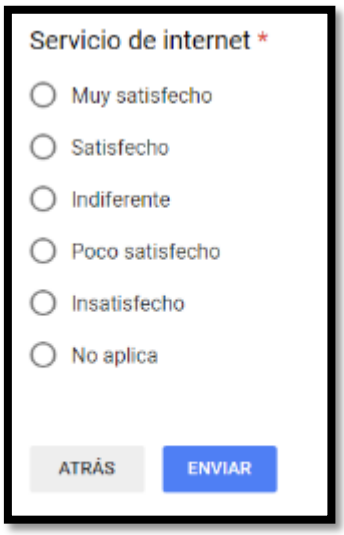


Figura 133 Diseño de encuesta cuarta parte
Elaborado por: Los autores.

De las encuestas que se realizaron se obtuvo los siguientes resultados:

1.- Fácil acceso a páginas institucionales:

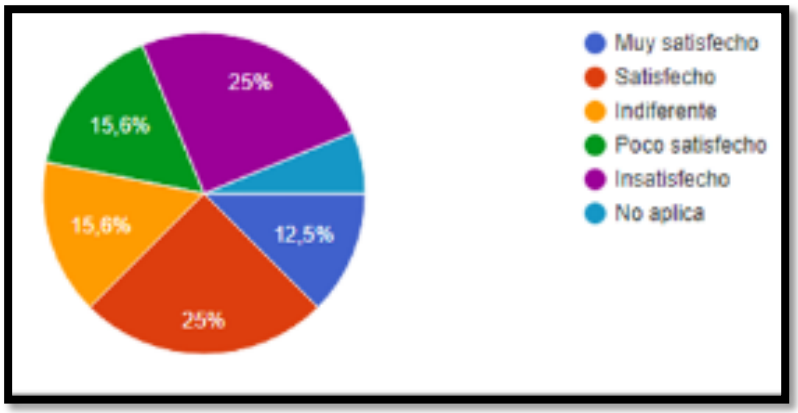


Figura 134. Resultado porcentual pregunta 1
Elaborado por: Los autores.

2.- Velocidad de Internet:

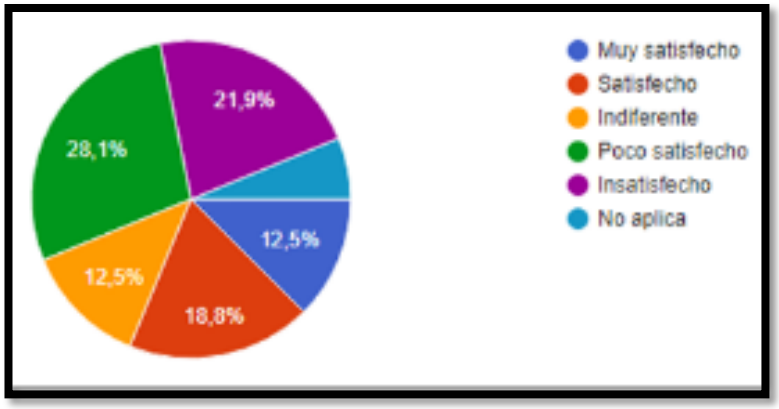


Figura 135 Resultado porcentual pregunta 2
Elaborado por: Los autores.

3.- Seguridad en navegación web:

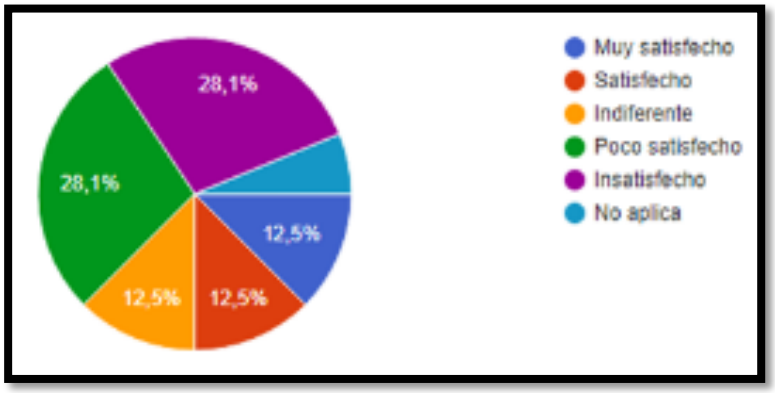


Figura 136 Resultado porcentual pregunta 3
Elaborado por: Los autores.

4.- Seguridad de correo institucional:

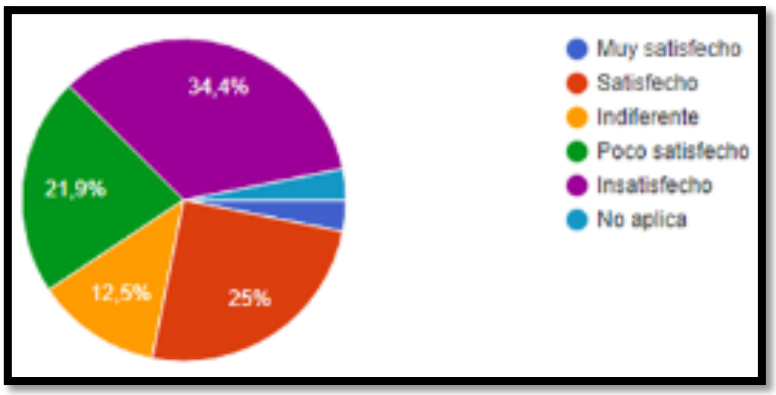


Figura 137 Resultado porcentual pregunta 4
Elaborado por: Los autores.

5.- Seguridad de la Información:

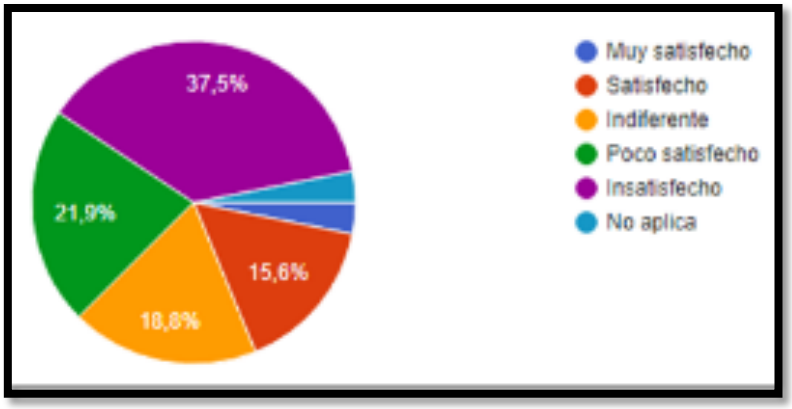


Figura 138 Resultado porcentual pregunta 5
Elaborado por: Los autores.

6.- Servicio de Internet:

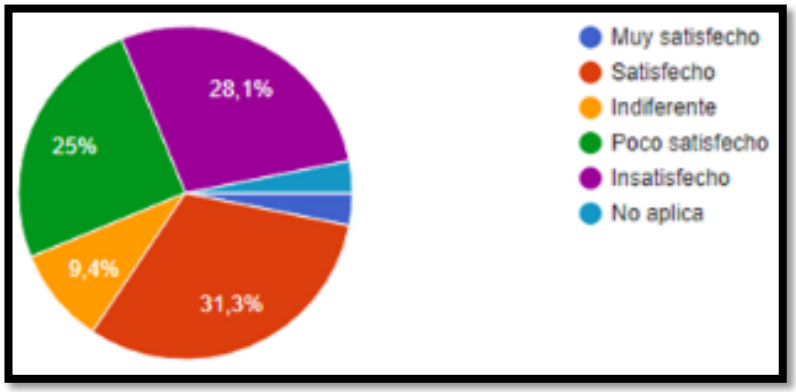


Figura 139 Resultado porcentual pregunta 6
Elaborado por: Los autores.

10.3. Anexo C: Instalación y configuración de NESSUS.

Para instalar NESSUS primero se registró de manera gratuita para una prueba de 7 días, Tenable enviará un correo para activar y registrar la cuenta para poder descargar el software.

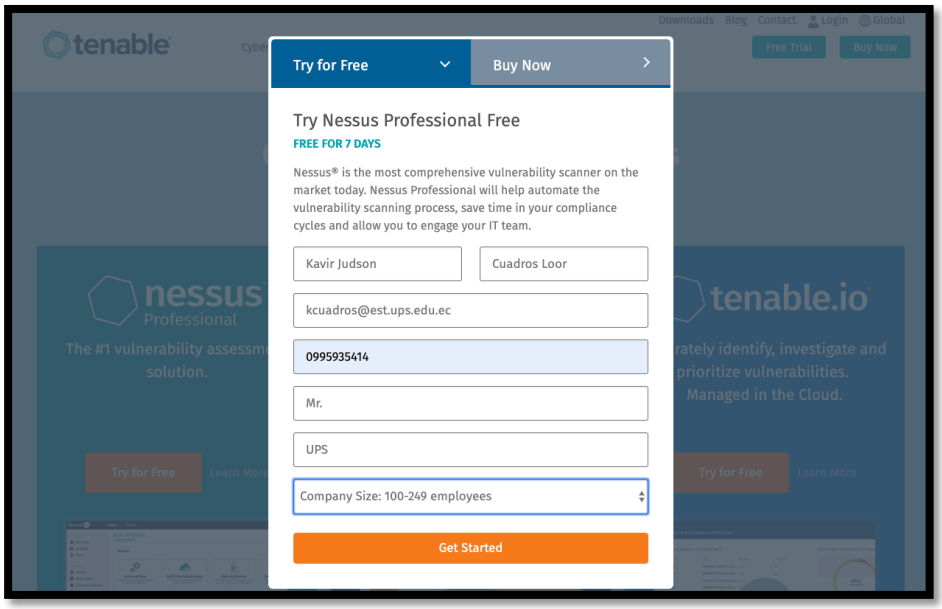


Figura 140. Registro en la página web para prueba de 7 días.
Elaborado por: Los autores.

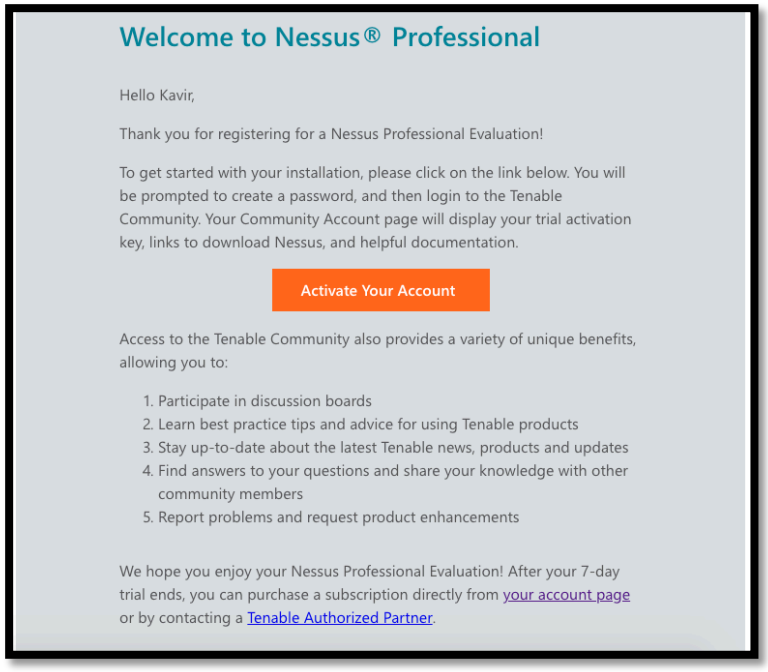


Figura 141. Correo para activar y crear cuenta.
Elaborado por: Los autores.

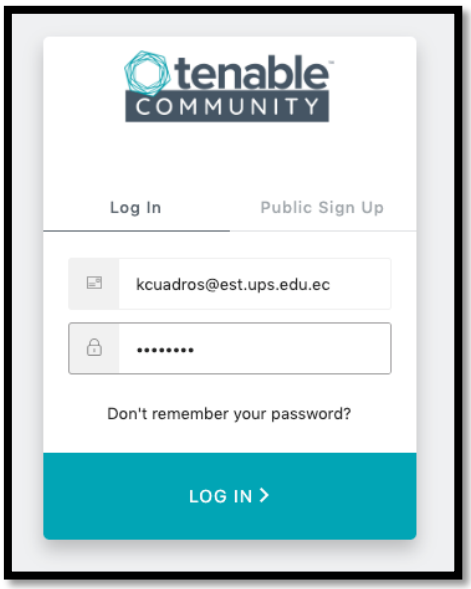


Figura 142. Inicio de sesión
Elaborado por: Los autores

.

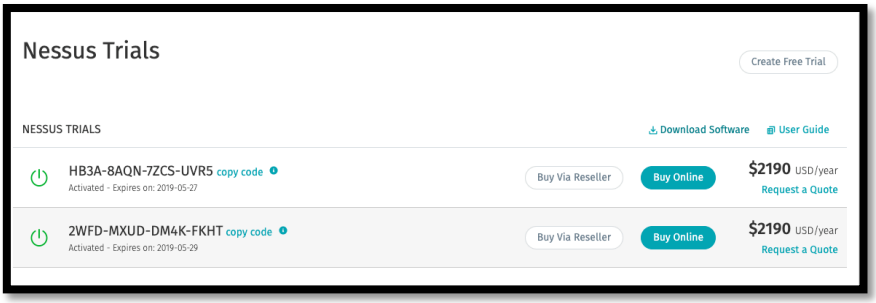


Figura 143. Página para descargar el Software y la licencia de prueba.
Elaborado por: Los autores.

Se ejecutó el instalador y aparecen las siguientes instrucciones y se continuará hasta finalizar la instalación.

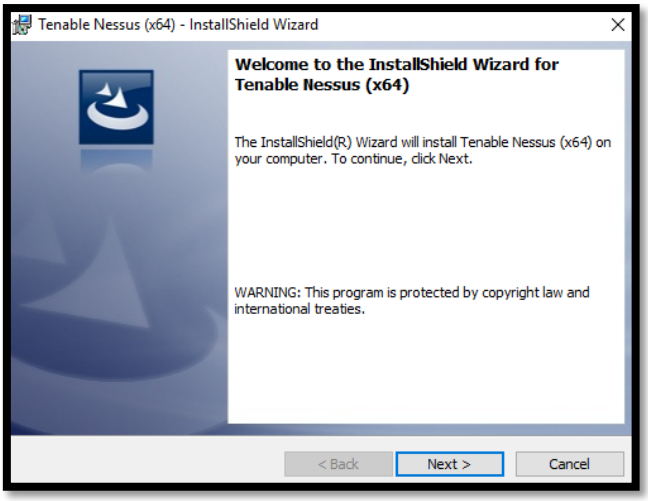


Figura 144. Comienzo de instalación de NESSUS.
Elaborado por: Los autores.

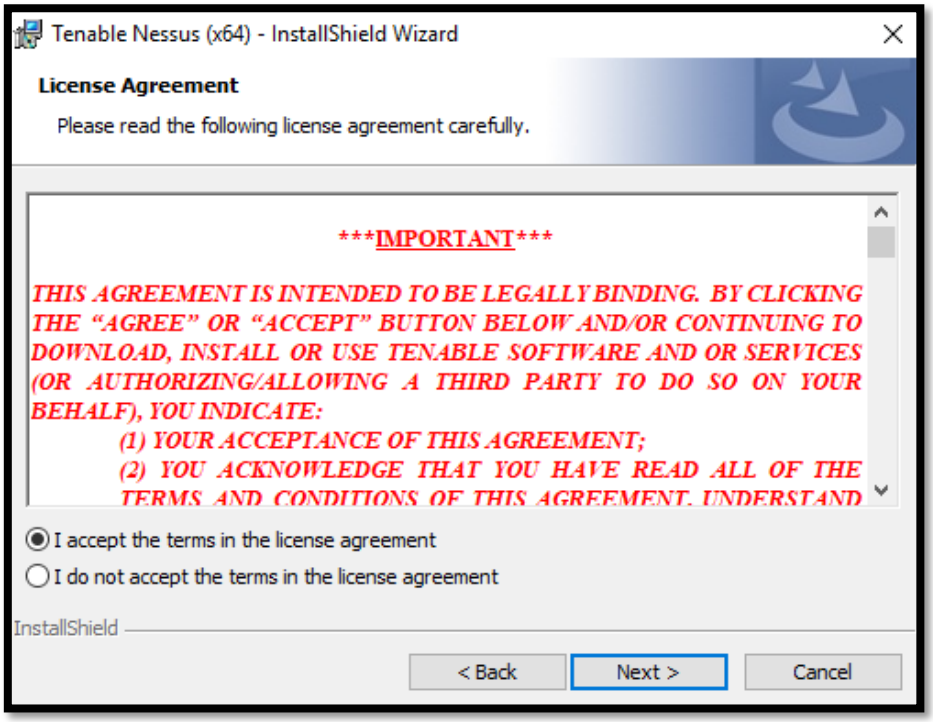


Figura 145. Aceptación de los términos de la licencia de NESSUS.
Elaborado por: Los autores.

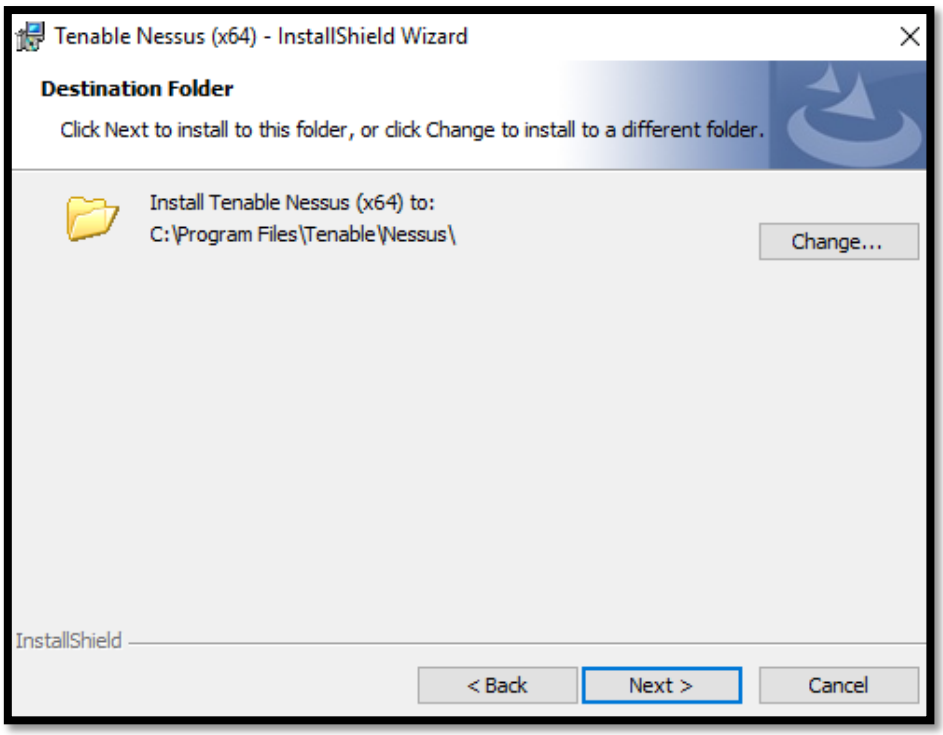


Figura 146. Selección de carpeta en la que se instalará NESSUS.
Elaborado por: Los autores.

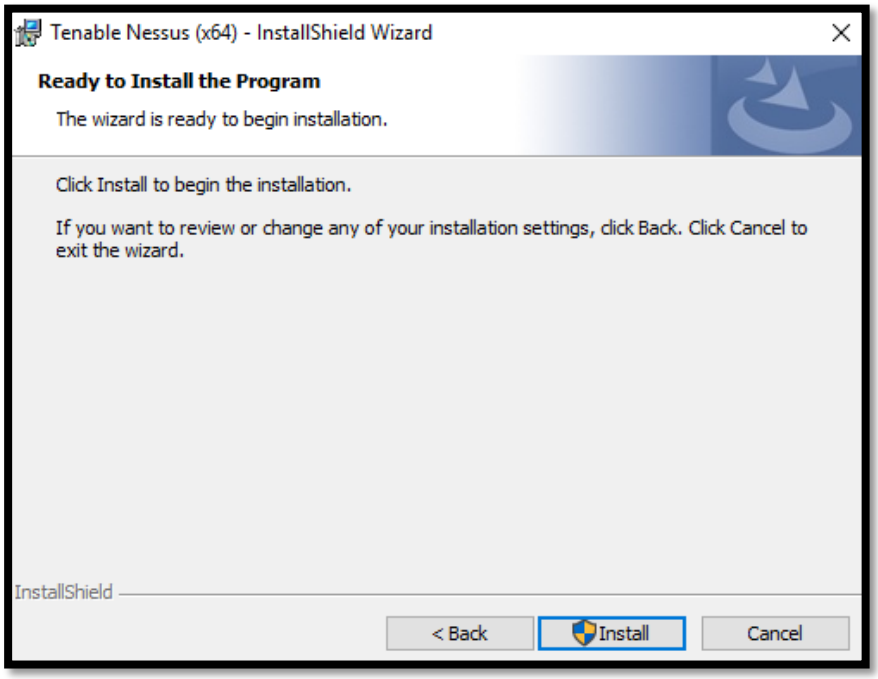


Figura 147. Autorización de la instalación de NESSUS.
Elaborado por: Los autores.

Una vez terminada la instalación se inicializa NESSUS en el navegador por defecto para realizar la conexión via SSL, se creará una cuenta para iniciar sesión y registrar la licencia.

Figura 148. Inicio de conexión vía SSL para NESSUS.
Elaborado por: Los autores.

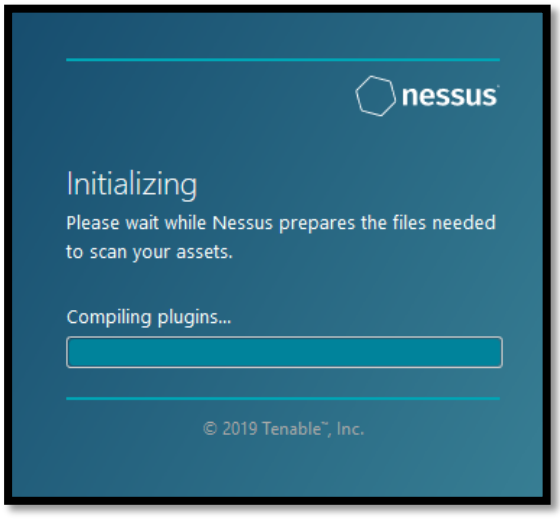


Figura 149. Inicialización de los componentes de NESSUS.
Elaborado por: Los autores.

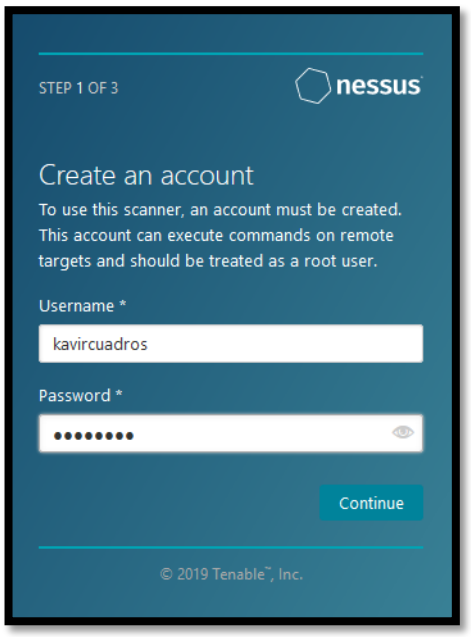


Figura 150. Creación de la cuenta en NESSUS.
Elaborado por: Los autores.

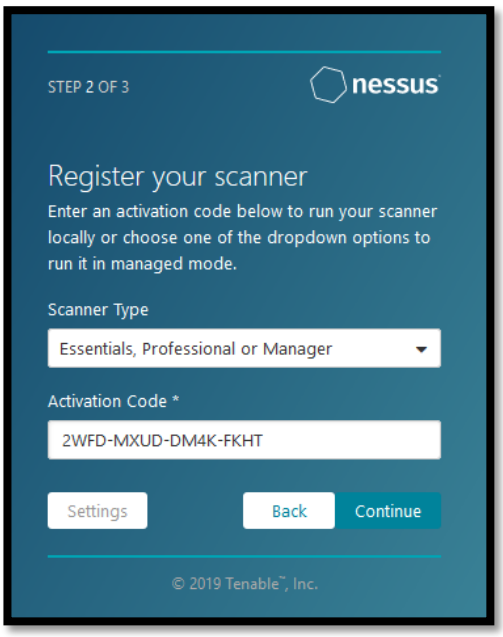


Figura 151. Registro de escáner con la licencia de NESSUS.
Elaborado por: Los autores

Una vez registrada la licencia, se puede crear políticas para el escaneo de vulnerabilidades o utilizar las plantillas que vienen por defecto, en este caso se utilizó la plantilla de escaneo avanzado y se define el rango IP.

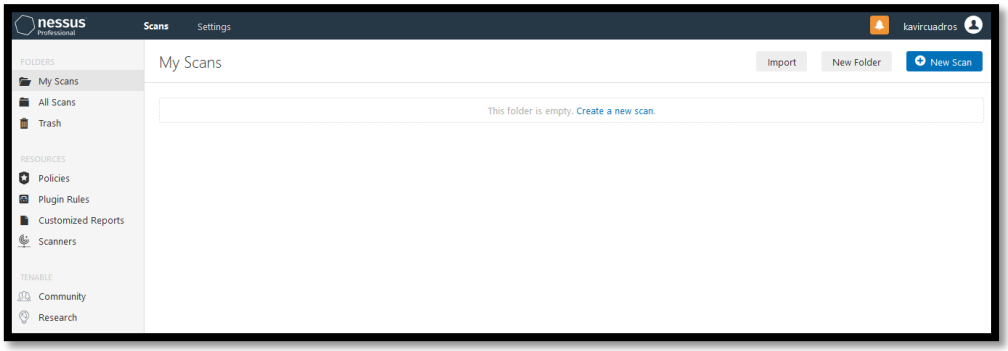


Figura 152. Dashboard inicial de NESSUS.
Elaborado por: Los autores.

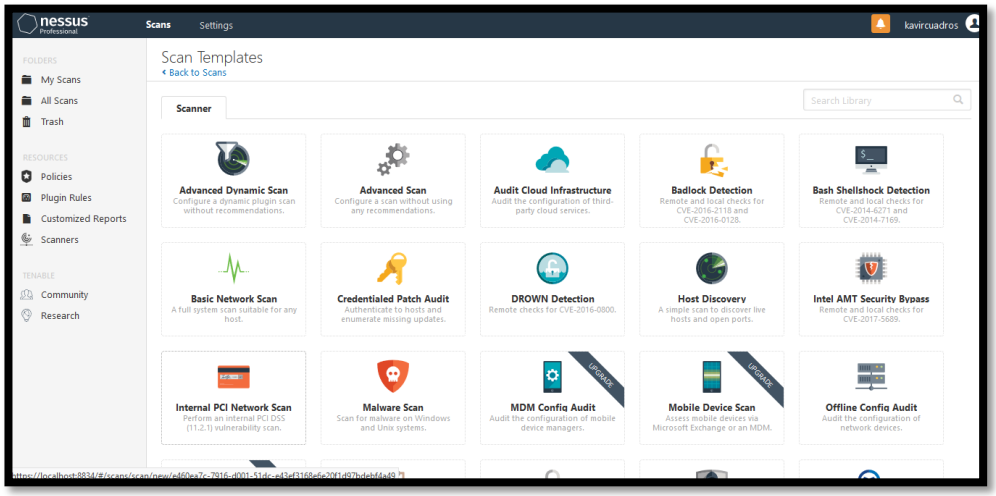


Figura 153. Plantilla de escaneo predefinidas en NESSUS.
Elaborado por: Los autores.

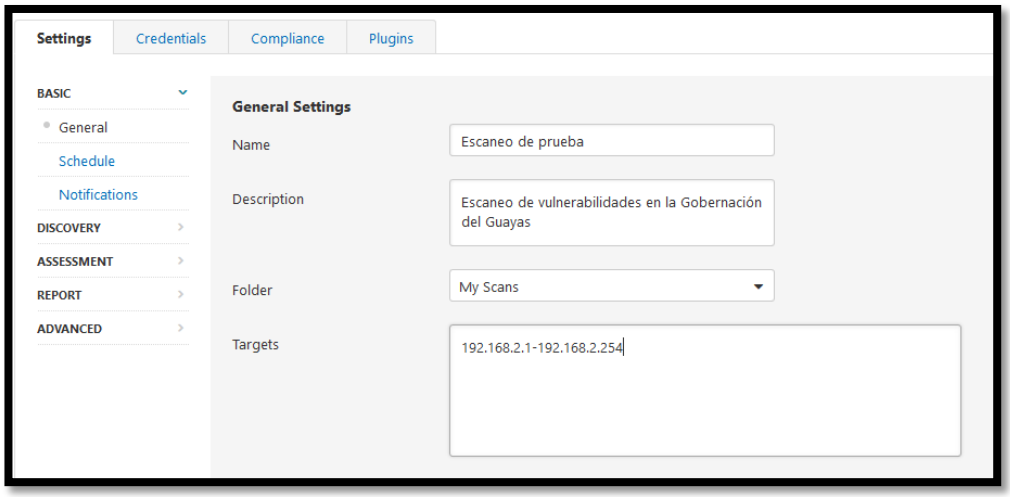


Figura 154. Configuración de escaneo en NESSUS.
Elaborado por: Los autores.

Figura 155. Inicio del escaneo en NESSUS.
Elaborado por: Los autores.

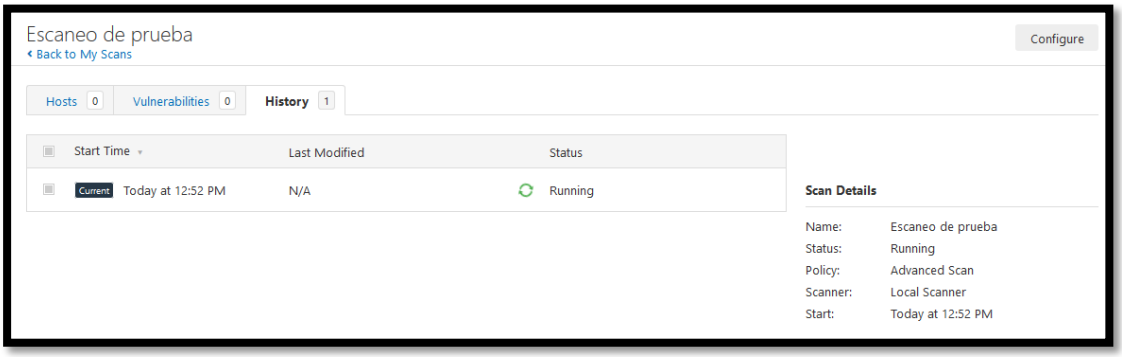


Figura 156. Escaneo en ejecución.
Elaborado por: Los autores.

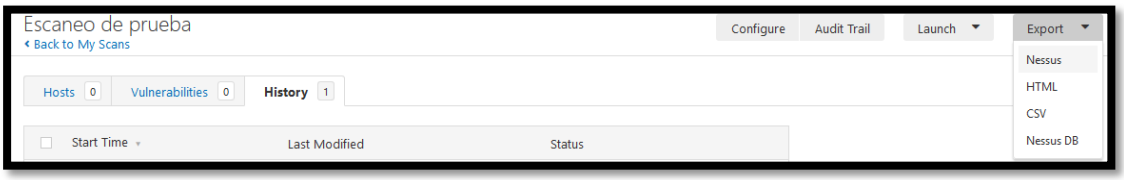


Figura 157. Visualizar resultado y exportarlo.
Elaborado por: Los autores.

10.4. Anexo D: Instalación y configuración de Active Directory

1. Agregar roles

Figura 158 Agregar roles al servidor
Elaborado por: Los autores

2. Seleccionar (Servicio de dominio de AD)

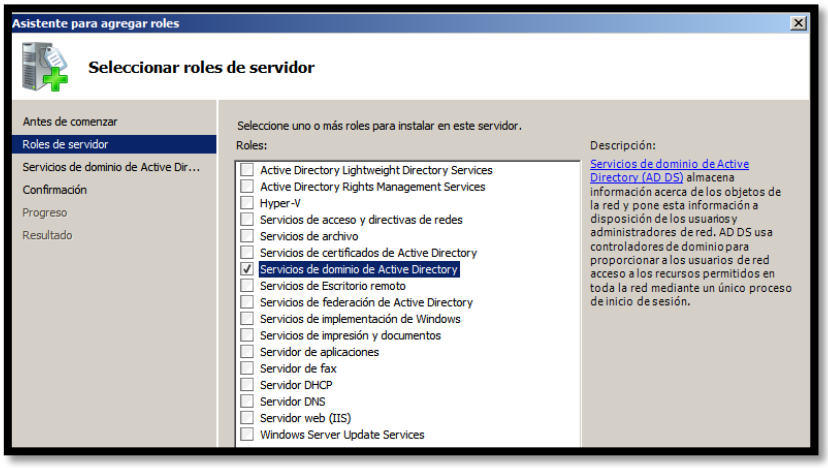


Figura 159 Seleccionar (Servicio de dominio de AD)
Elaborado por: Los autores

3. Introducción de Active Directory

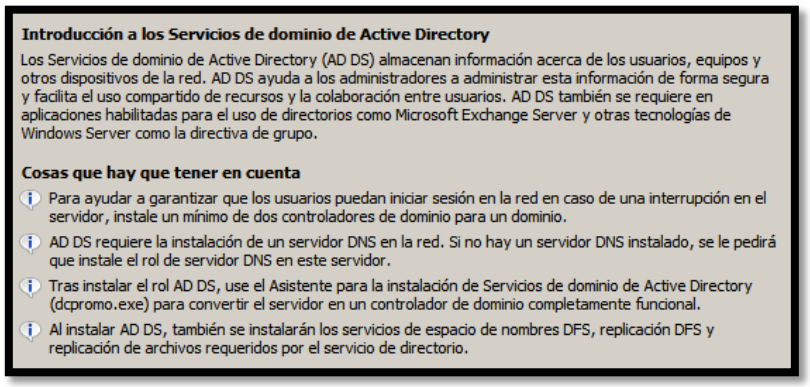


Figura 160 Introducción de Active Directory
Elaborado por: Los autores

4. Detalle de lo que se instalará

Figura 161 Detalle de la Instalación
Elaborado por: Los autores

5. Resumen de la instalación

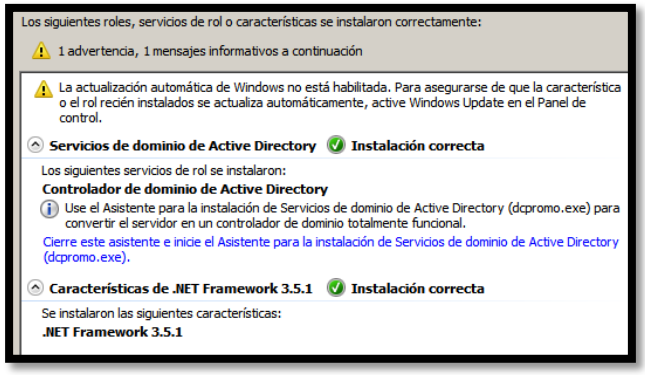


Figura 162 Resumen de la instalación
Elaborado por: Los autores

6. Servicios de dominio de AD

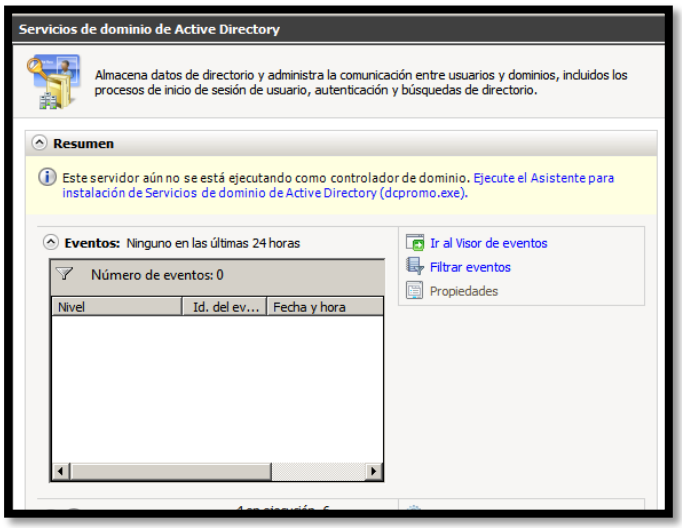


Figura 163 Configuración del servicio de dominio
Elaborado por: Los autores

7. Asignación de IP fija

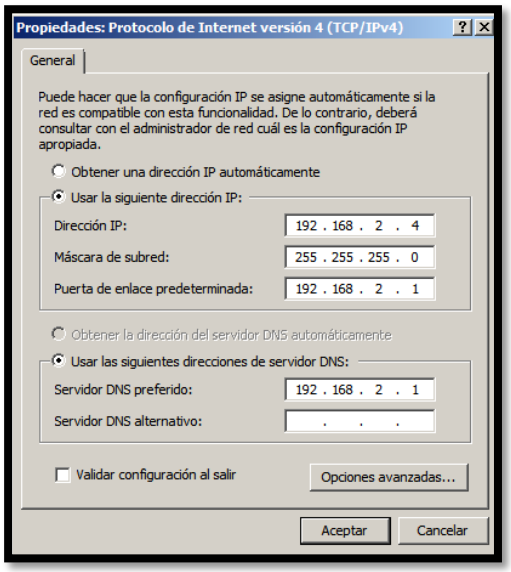


Figura 164 Asignación de IP fija
Elaborado por: Los autores

8. Se abre el asistente para instalar los Servicios de domino de Active Directory.

Figura 165 Asistente para la instalación de servicios de dominio de AD
Elaborado por: Los autores

9. Se selecciona la opción para crear un domino nuevo en un bosque nuevo.

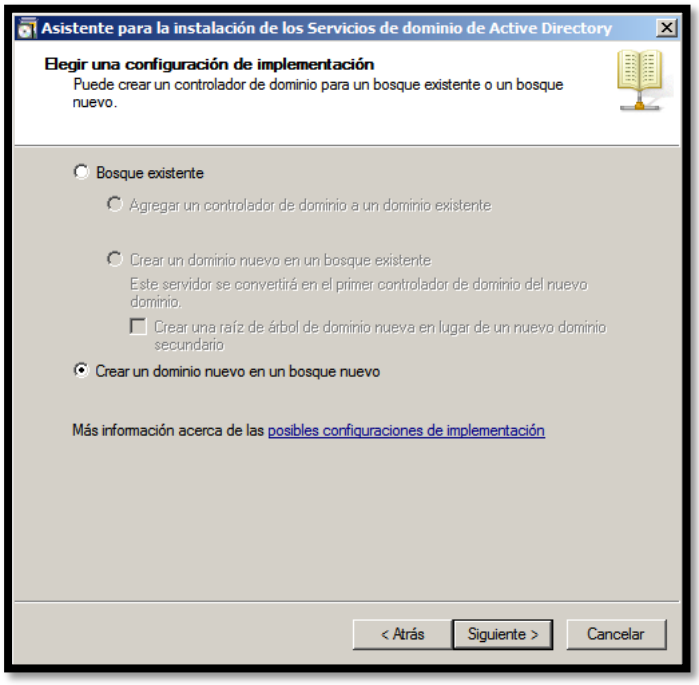


Figura 166 Creación de dominio en bosque nuevo
Elaborado por: Los autores

10. Nombre NetBIOS predeterminado

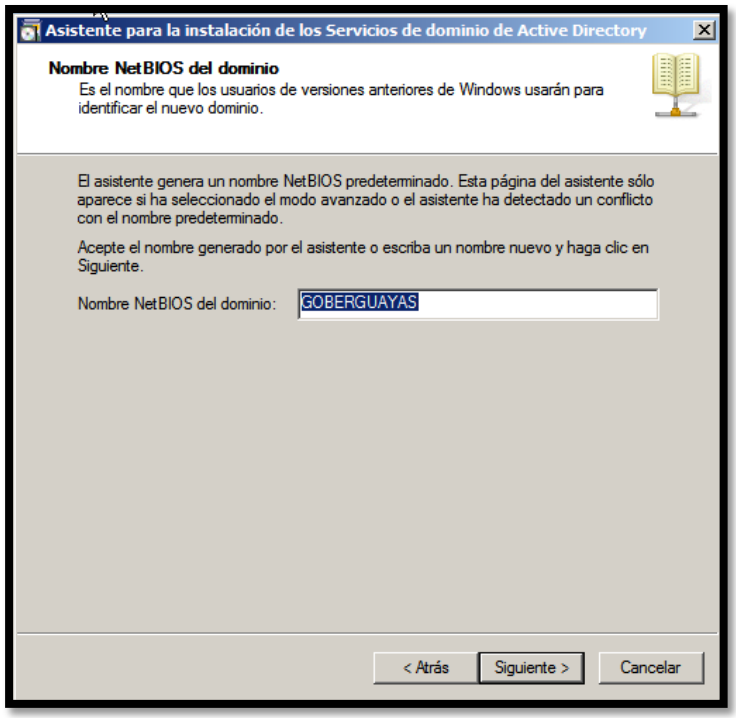


Figura 167 Nombre de NetBIOS del dominio
Elaborado por: Los autores

11. Elegir nivel funcional del bosque.

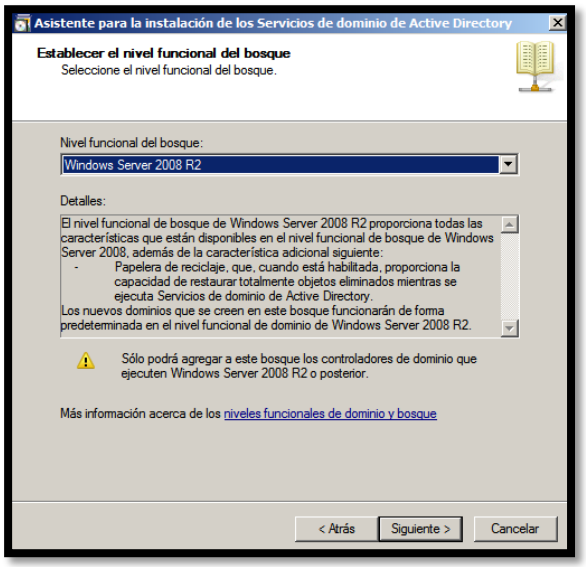


Figura 168 Nivel funcional del bosque
Obtenido de: Windows Server 2008 R2

12. Seleccionar opciones de DNS

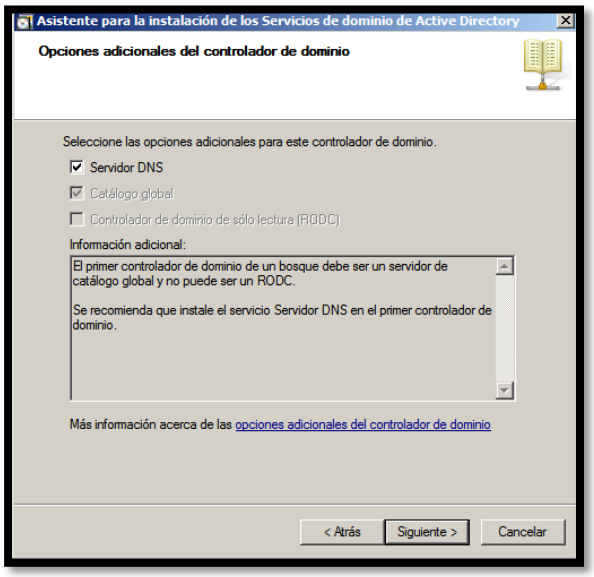


Figura 169 Selección de servidor DNS
Obtenido de: Windows Server 2008 R2

13. Base de datos

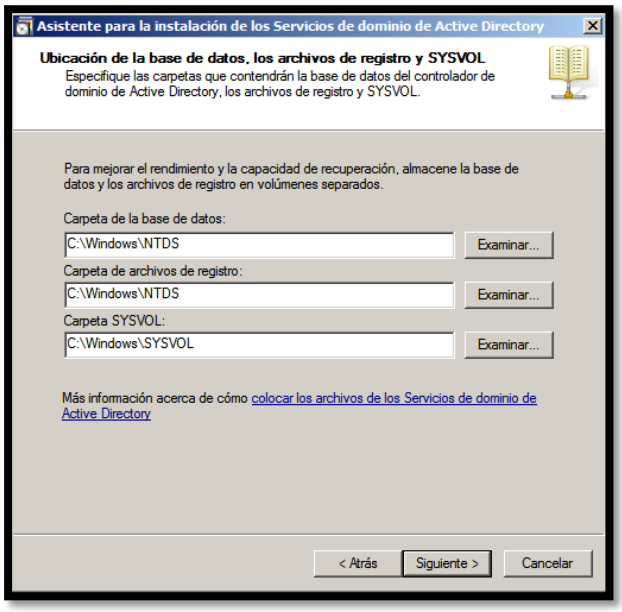


Figura 170 Base de datos
Obtenido de: Windows Server 2008 R2

14. Contraseña

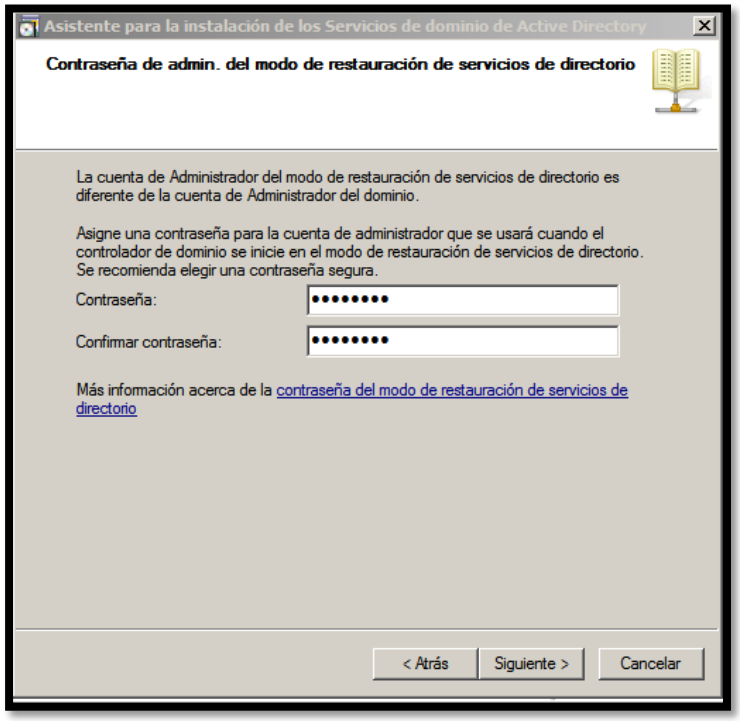


Figura 171 Contraseña de administrador del dominio
Obtenido de: Windows Server 2008 R2

15. Resumen de configuración

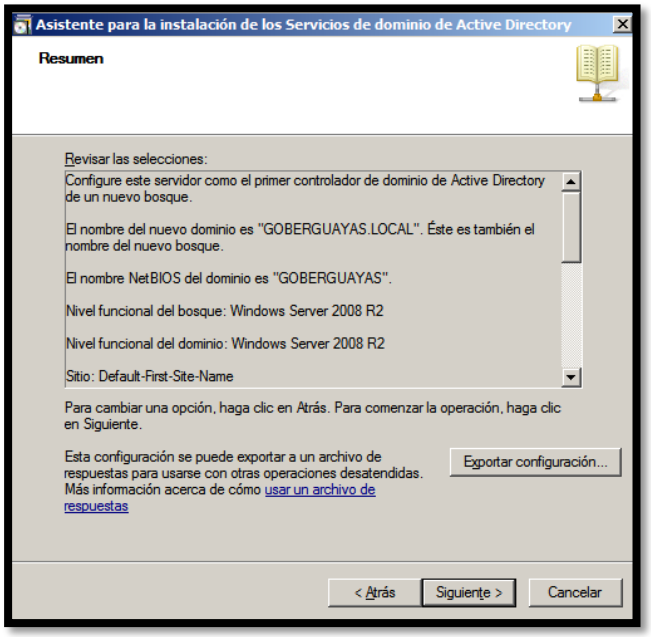


Figura 172 Resumen de la configuración
Obtenido de: Windows Server 2008 R2

16. Configurando

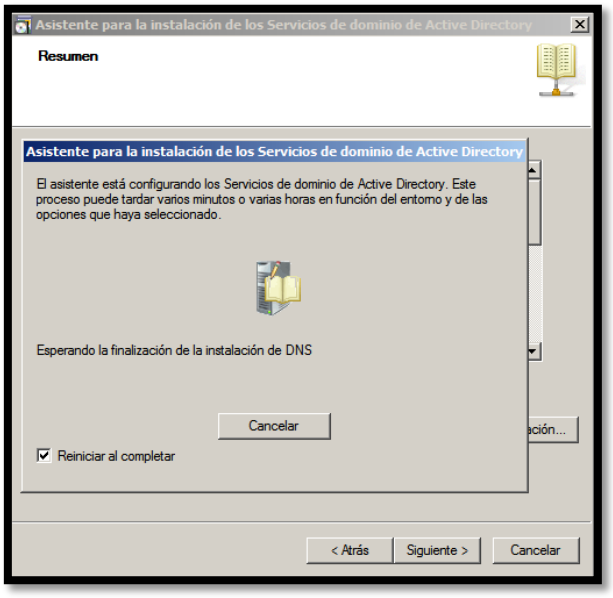


Figura 173 Configuración del servidor
Obtenido de: Windows Server 2008 R2

- **Creación de Unidades Organizativas**

Se configuró Gobernación como Unidad Organizativa principal y dentro de la misma se creó equipos y usuarios para la configuración de estos.

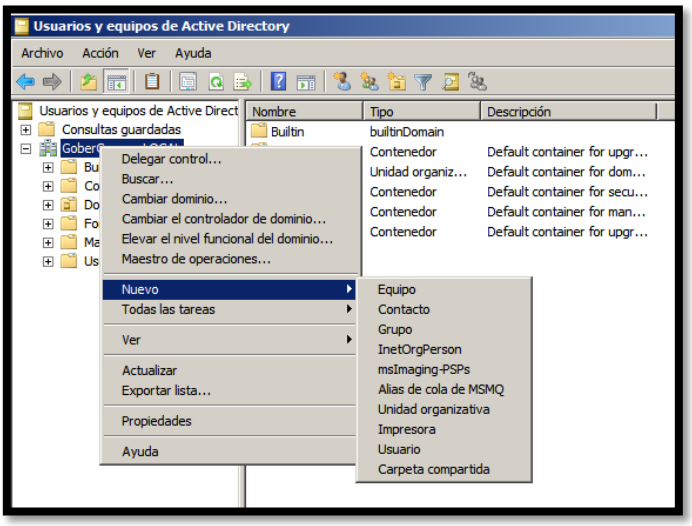


Figura 174. Crear nueva Unidad Organizativa.
Elaborado por: Los autores.

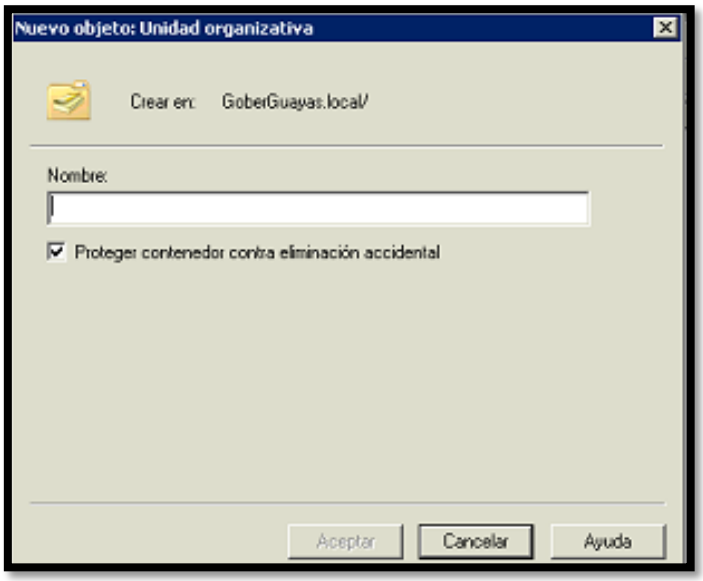


Figura 175. Nombrar Unidad Organizativa.
Elaborado por: Los autores.

- **Creación de equipos dentro de la Unidad Organizativa**

En la Unidad Organizativa “Equipos” se añadió todos los departamentos existentes que tienen acceso a la red, así mismo, en cada departamento se añadió los equipos de cómputo.

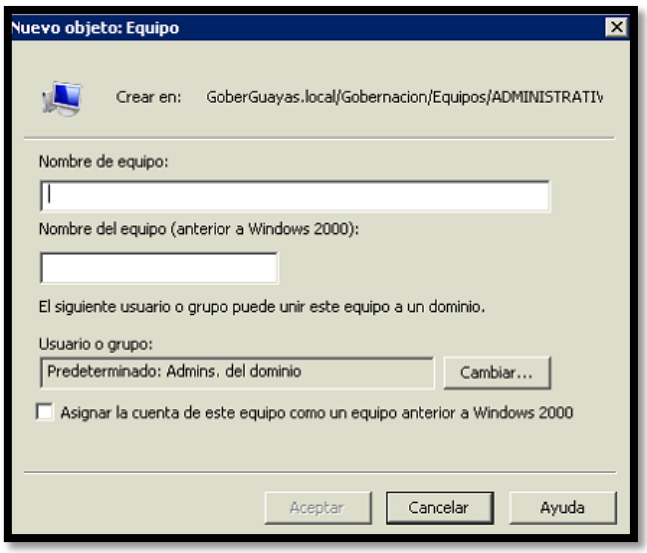


Figura 176. Creación de Equipo
Elaborado por: Los autores.

- **Creación de usuarios dentro de la Unidad Organizativa**

En la Unidad Organizativa “Usuarios” se añadió todos los departamentos existentes que tienen acceso a la red, así mismo, en cada departamento se añadió los usuarios.

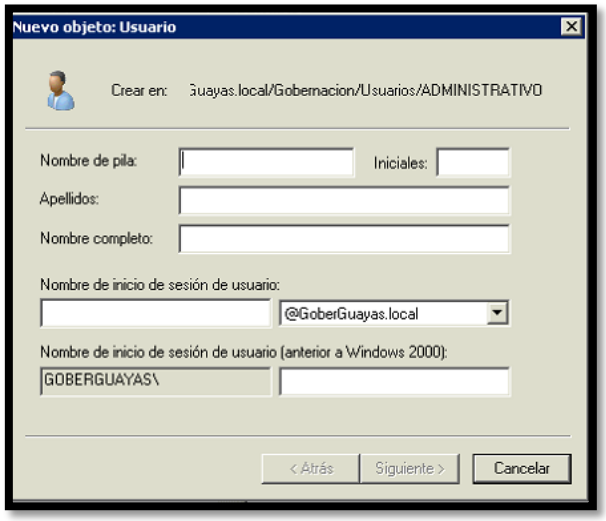


Figura 177. Creación de usuario.
Elaborado por: Los autores.

- **Creación de grupos**

En las Unidades Organizativas de usuarios por departamento se creó un grupo exclusivo para compartición de carpetas.

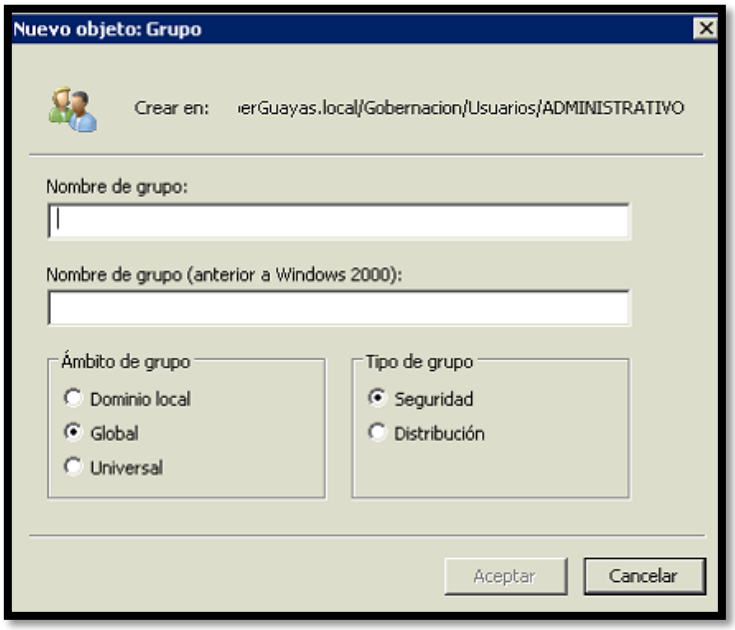


Figura 178. Creación de grupo
Elaborado por: Los autores.

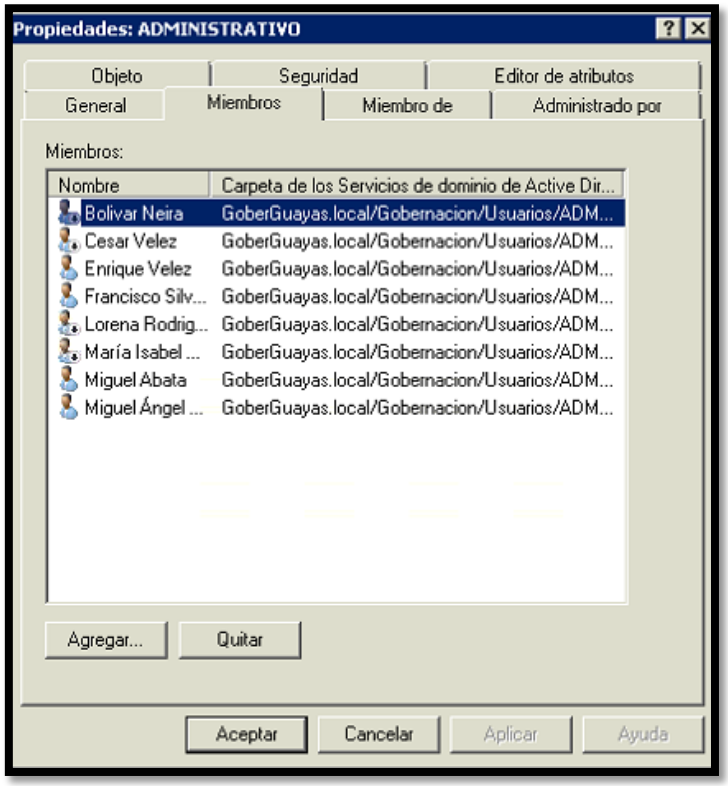


Figura 179. Agregar miembros al grupo.
Elaborado por: Los autores.

- **Creación de políticas**

En la administración de directivas de grupo se creó una nueva GPO donde se definió todas las políticas para el manejo de usuarios y equipos con acceso al domino.

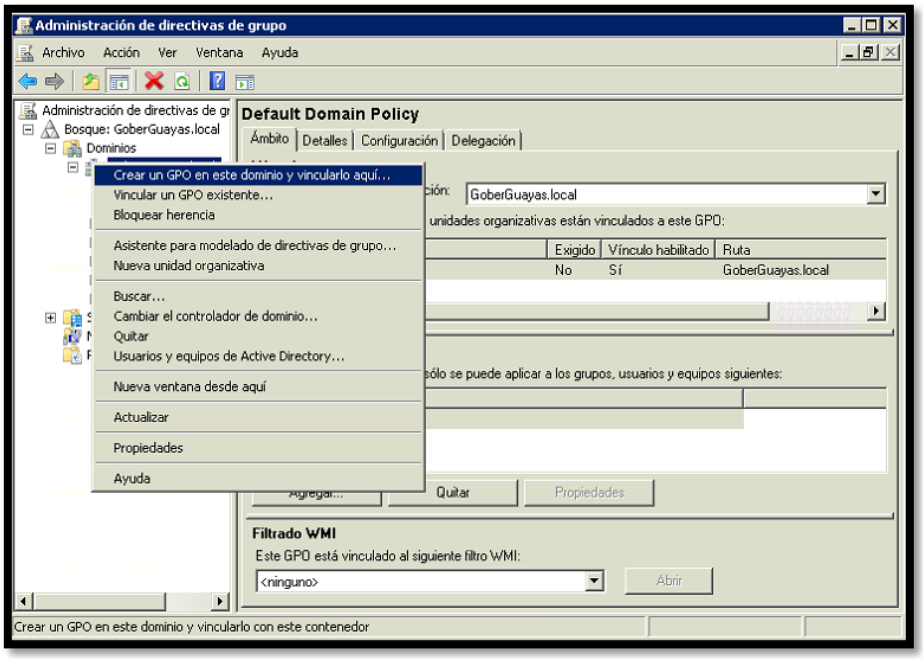


Figura 180. Creación de GPO para el dominio.
Elaborado por: Los autores.

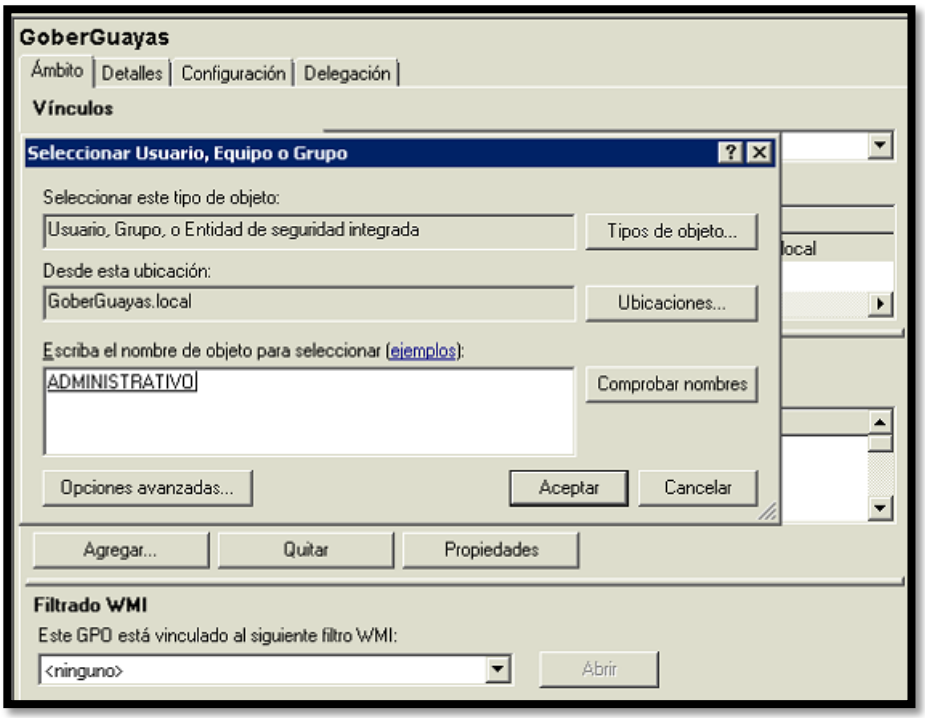


Figura 181. Añadir grupos a los que se aplicará las políticas.
Elaborado por: Los autores.

Una vez agregados los usuarios se editaron las políticas, donde se definieron los accesos a configuraciones del sistema que tendrán acceso los usuarios, como panel de control, entre otras.

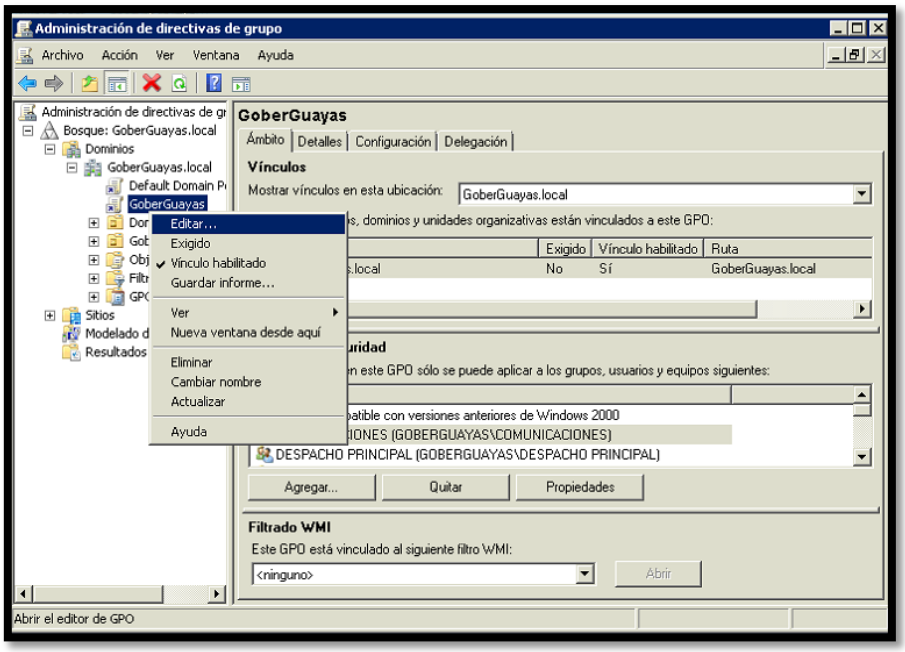


Figura 182. Edición de políticas.
Elaborado por: Los autores.

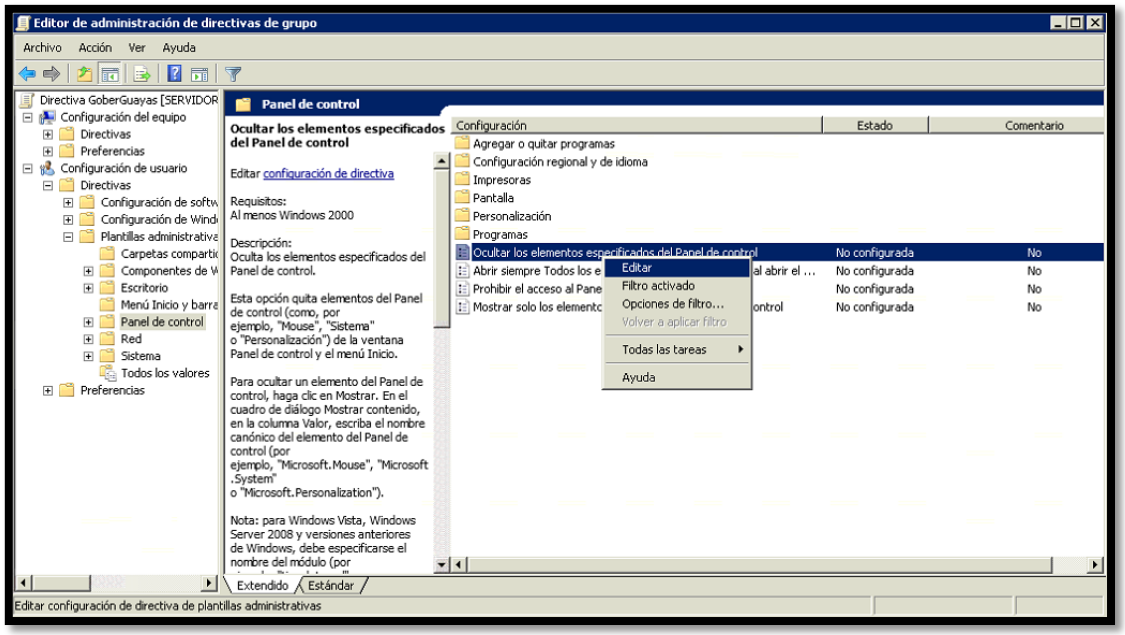


Figura 183. Edición de políticas en panel de control.
Elaborado por: Los autores.

10.5. Anexo E: Instalación y configuración de Sophos.

El equipo UTM Sophos SG 210 viene preinstalado con su software, para las configuraciones iniciales se debe conectar un monitor al dispositivo para asignar la red lan y su respectiva IP. Se accede desde un equipo dentro de la red por medio de un navegador, la dirección es: https://192.168.2.1:4444.

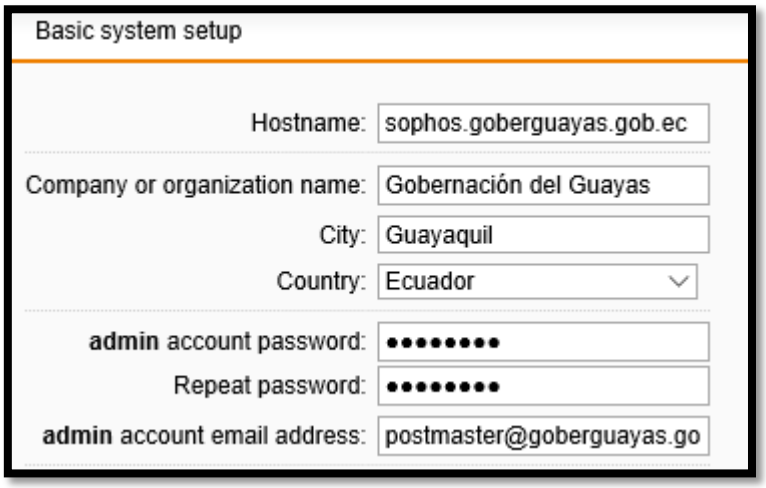


Figura 184. Configuración básica
Elaborado por: Los autores.

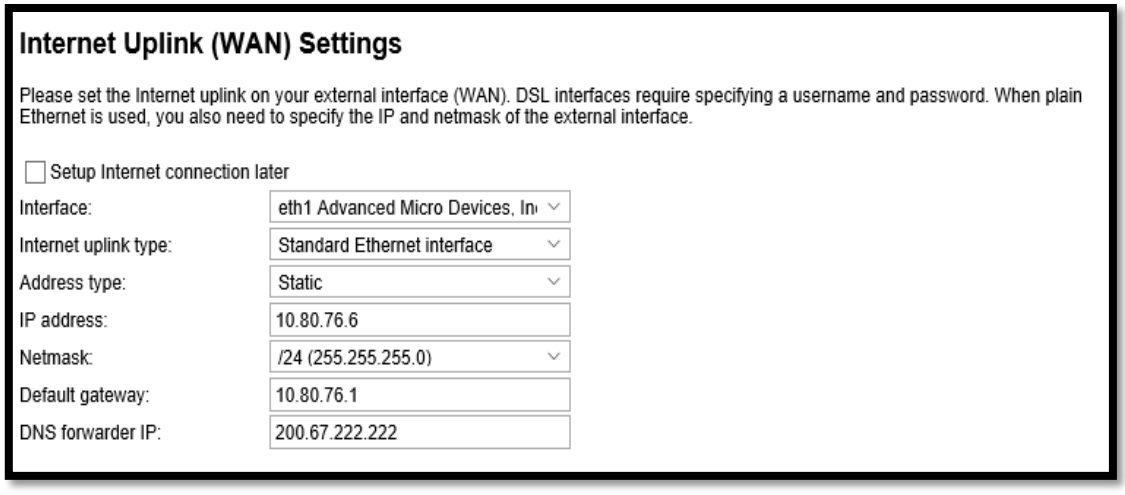


Figura 185. Configuración de WAN.
Elaborado por: Los autores.

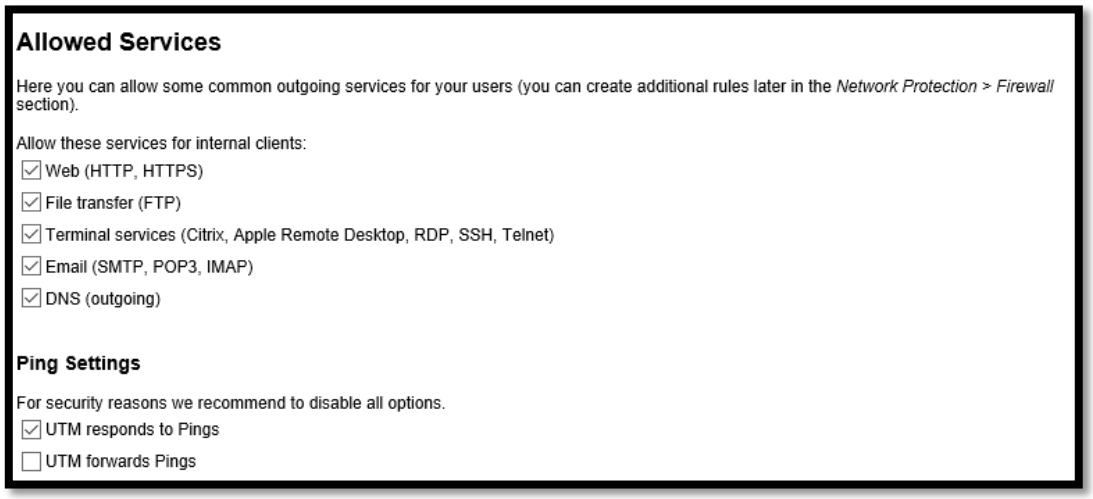


Figura 186. Selección de servicios levantados.
Elaborado por: Los autores.

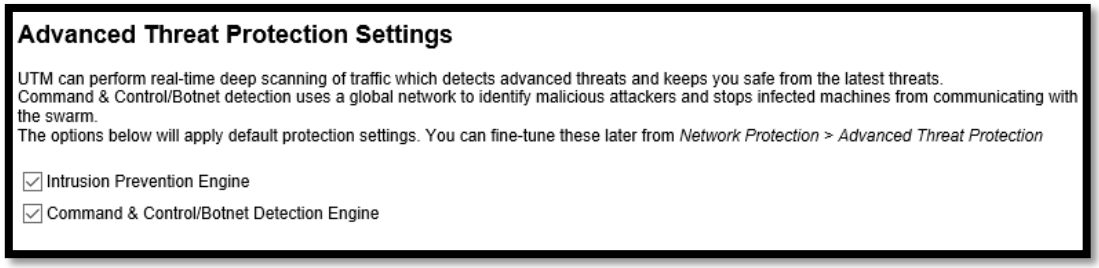


Figura 187. Activación de la Protección contra intrusos.
Elaborado por: Los autores.

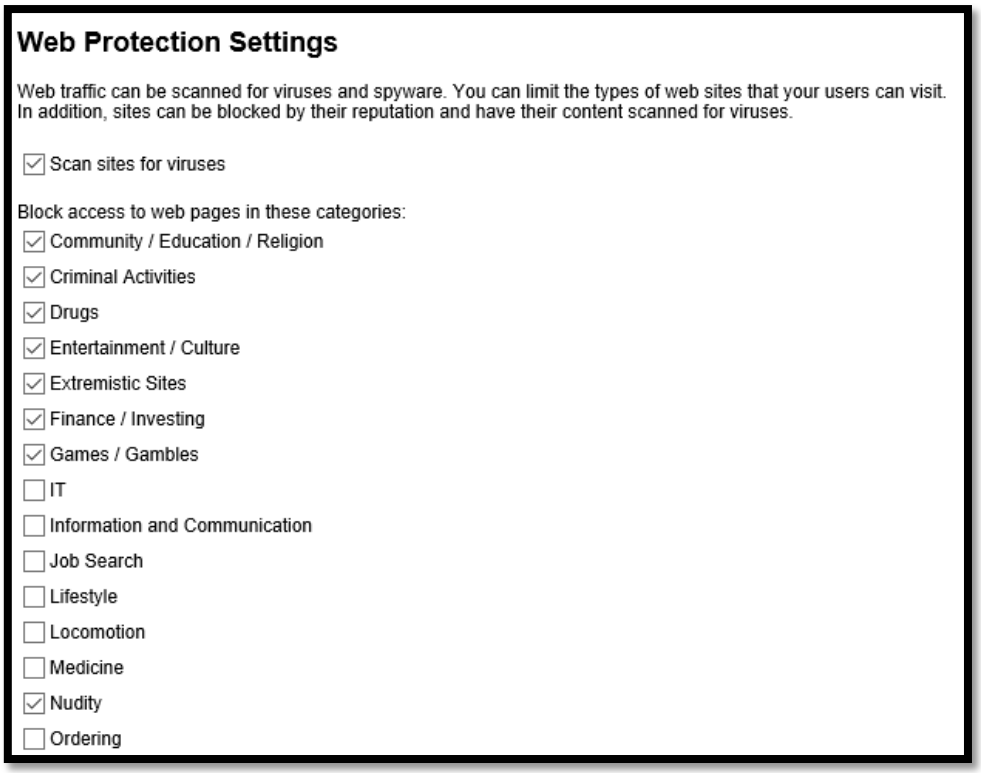


Figura 188. Activación de las principales protecciones web.
Elaborado por: Los autores.

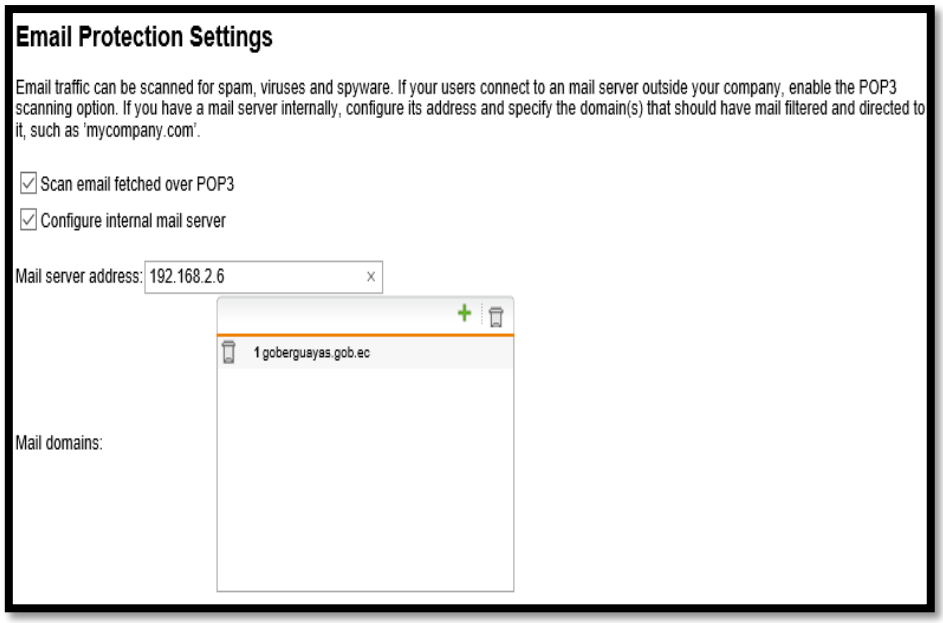


Figura 189. Configuración de Protección de Correo.
Elaborado por: Los autores.

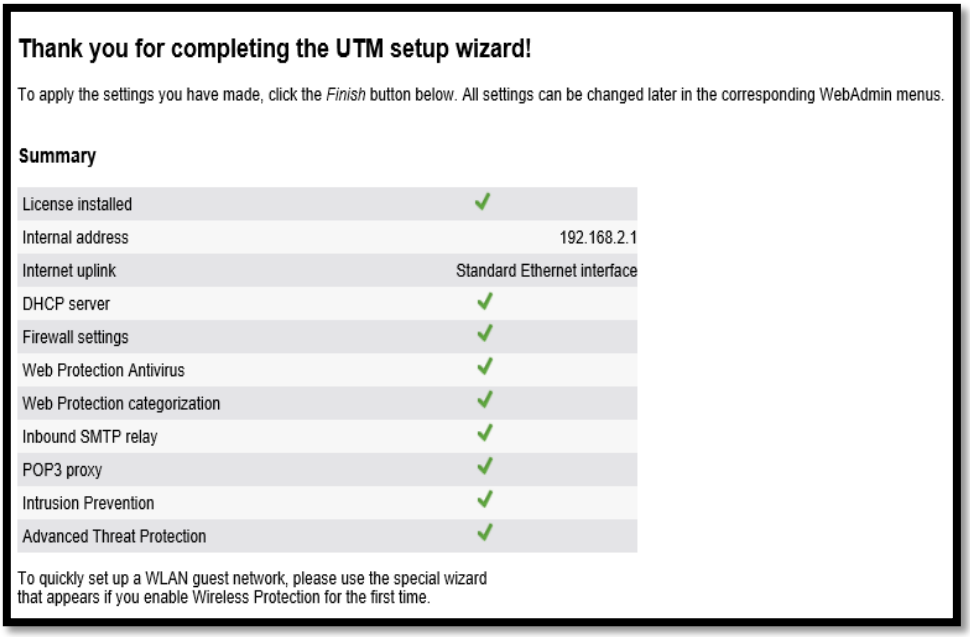


Figura 190. Resumen de configuraciones realizadas.
Elaborado por: Los autores.

- **Configuraciones Network Services**

En el módulo DNS se configuró las redes que serán permitidas a usar Sophos UTM como DNS recursivo, DNS forwarder y el DNS del servidor de domino.

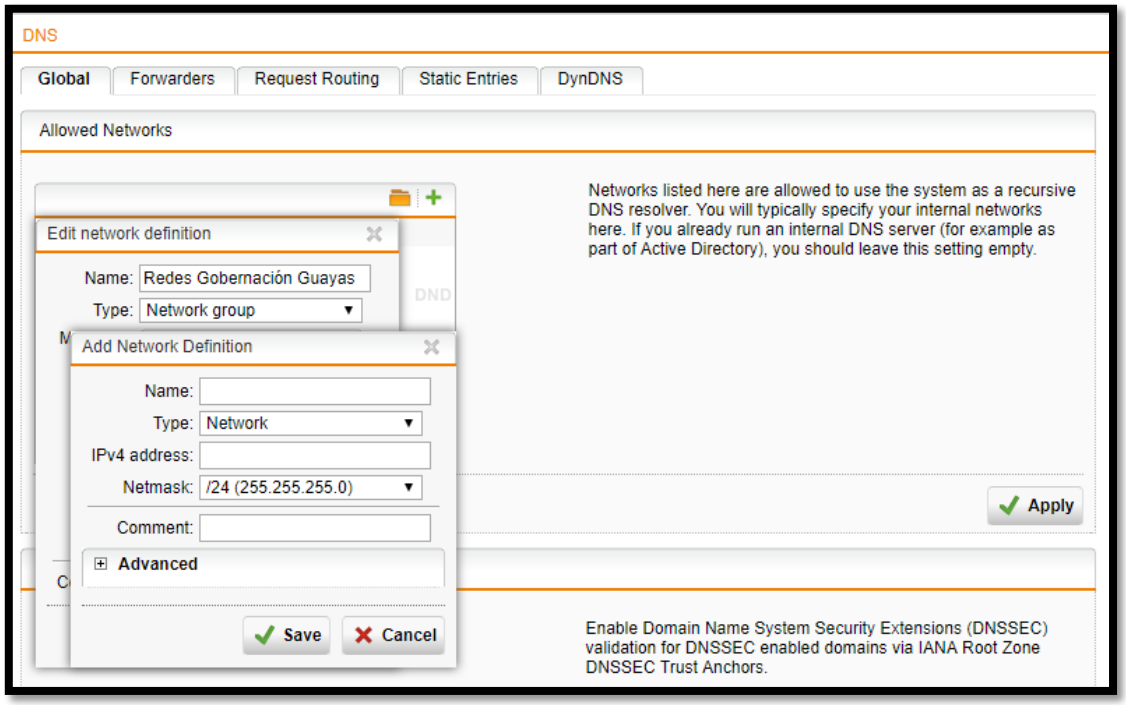


Figura 191. Agregar redes permitidas por DNS.
Elaborado por: Los autores.

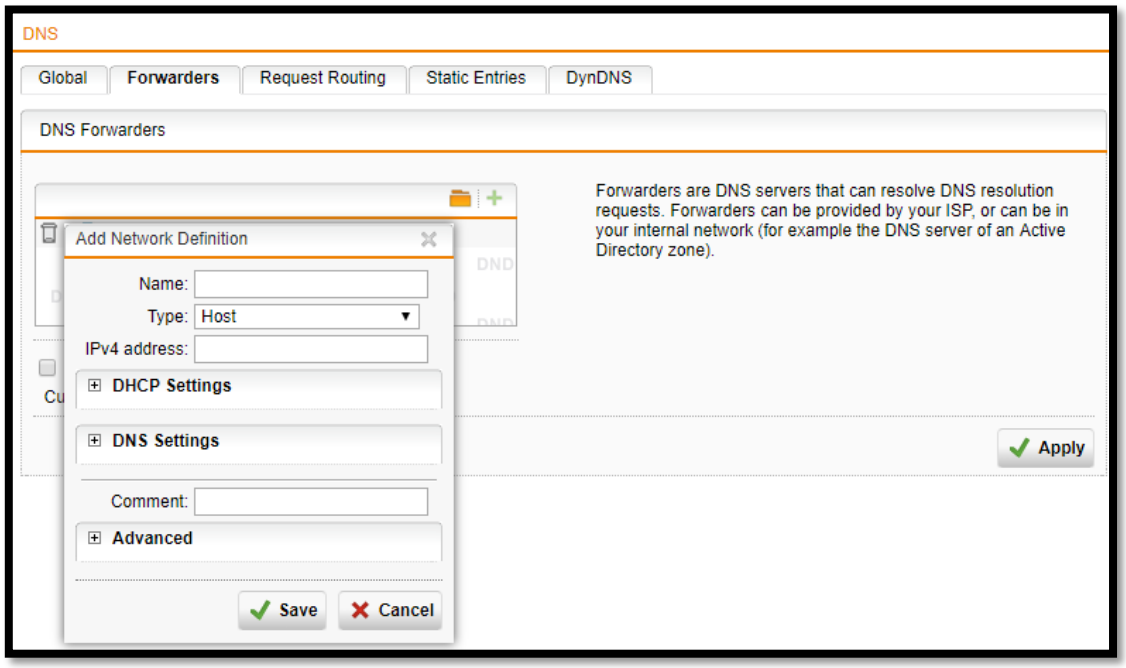


Figura 192. Agregar DNS forwarder
Elaborado por: Los autores.

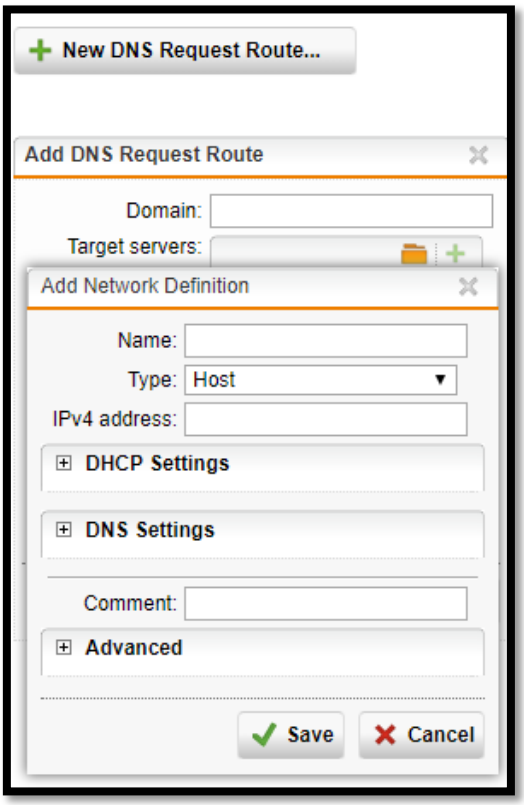


Figura 193. Agregar DNS interno
Elaborado por: Los autores.

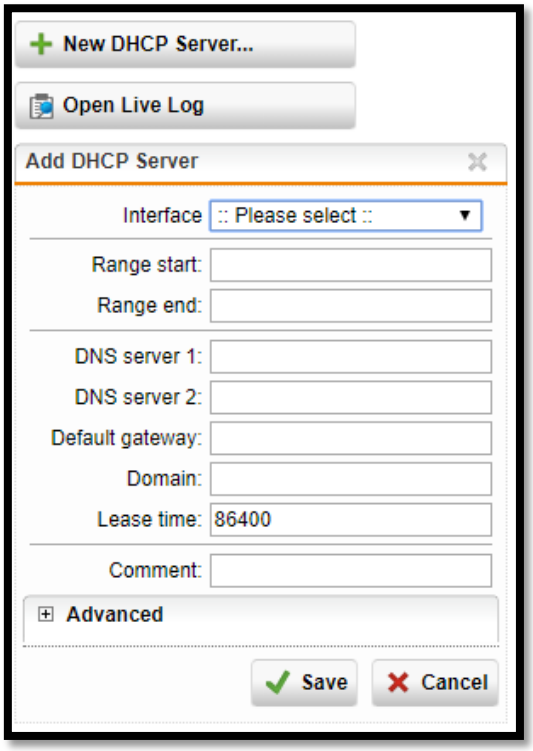


Figura 194. Agregar rango DHCP
Elaborado por: Los autores.

- **Configuraciones Network Protection**

En este módulo se configuró para la protección de la red mediante reglas de firewall, excepciones de acceso, masquerading, NAT y añadir el servicio VoIP.

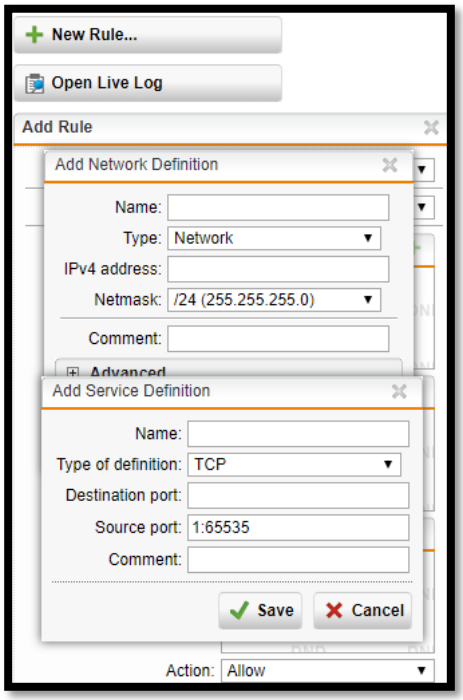


Figura 195. Agregar reglas de firewall
Elaborado por: Los autores.

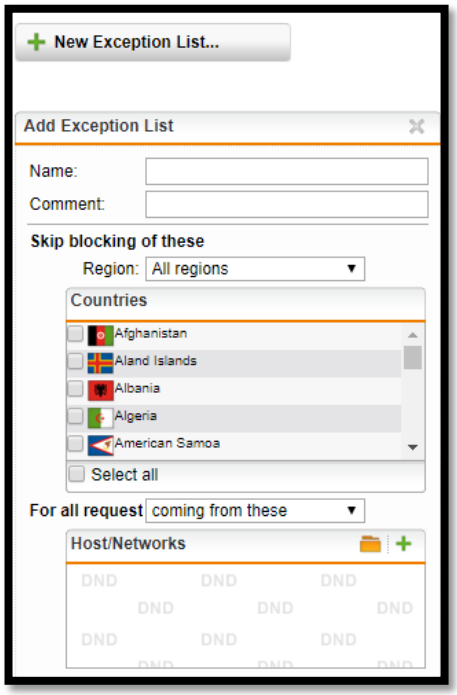


Figura 196. Agregar países a bloquear.
Elaborado por: Los autores.

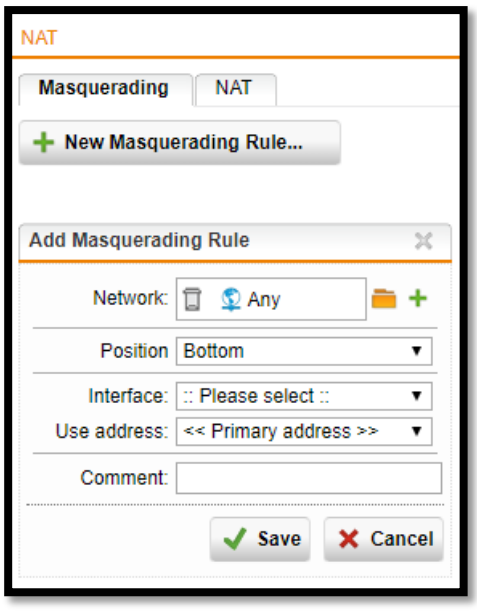


Figura 197. Agregar reglas masquerading,
Elaborado por: Los autores.

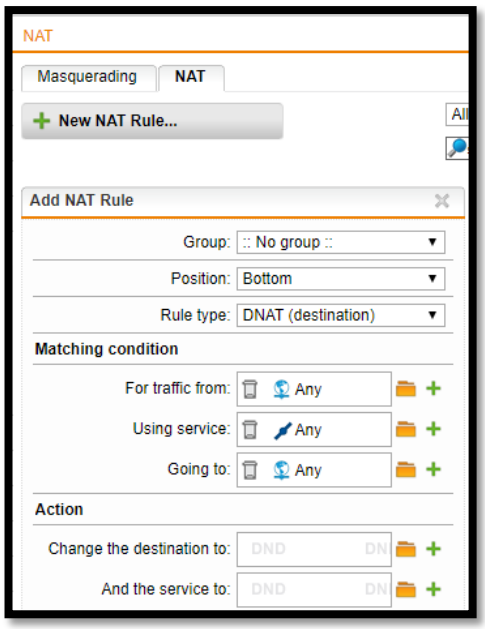


Figura 198. Agregar reglas NAT.
Elaborado por: Los autores.

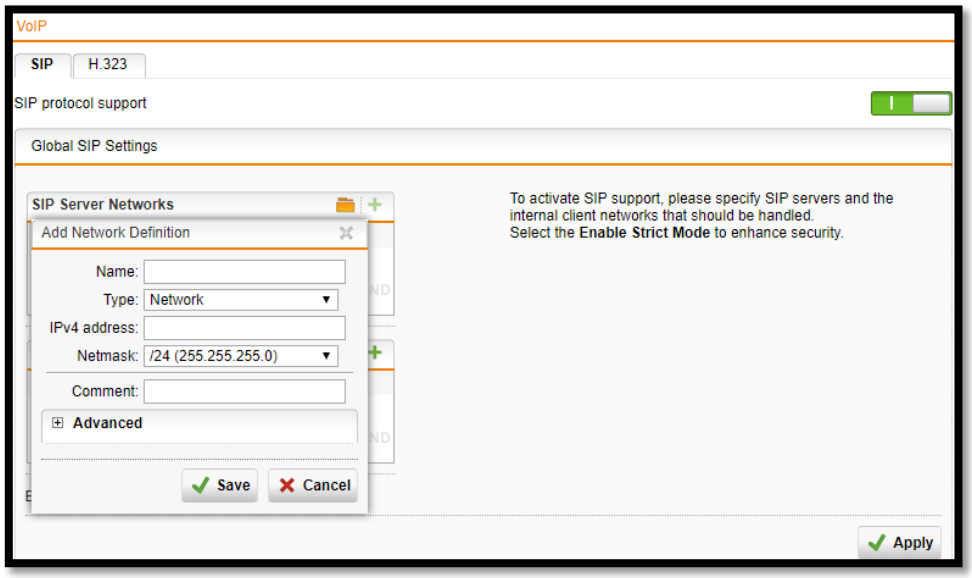


Figura 199. Agregar servidor VoIP
Elaborado por: Los autores.

- **Configuraciones Web Protection**

En este módulo se configuró las redes que pasaran por el filtrado web, las reglas para usuarios y grupos específicos, las políticas para navegación web y el control de aplicaciones.

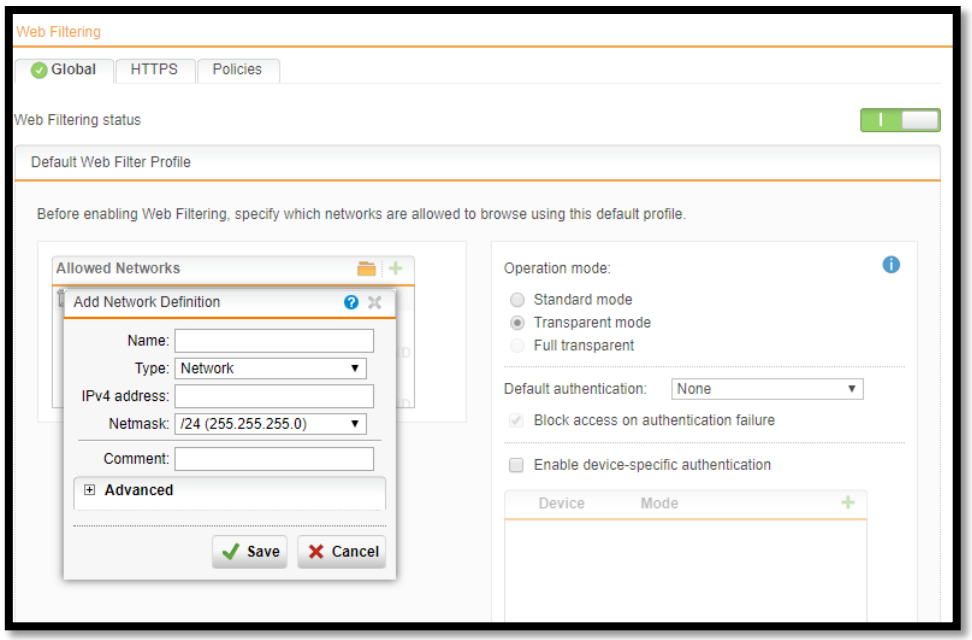


Figura 200. Agregar red para filtrado web.
Elaborado por: Los autores.

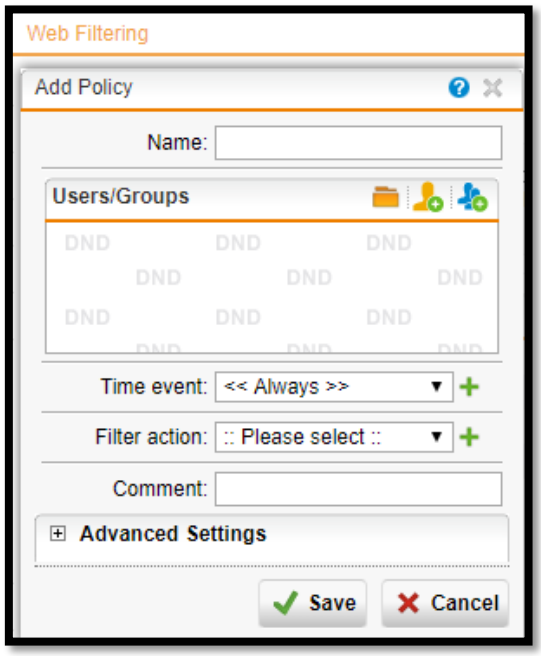


Figura 201. Agregar politica para grupos y usuarios.
Elaborado por: Los autores.

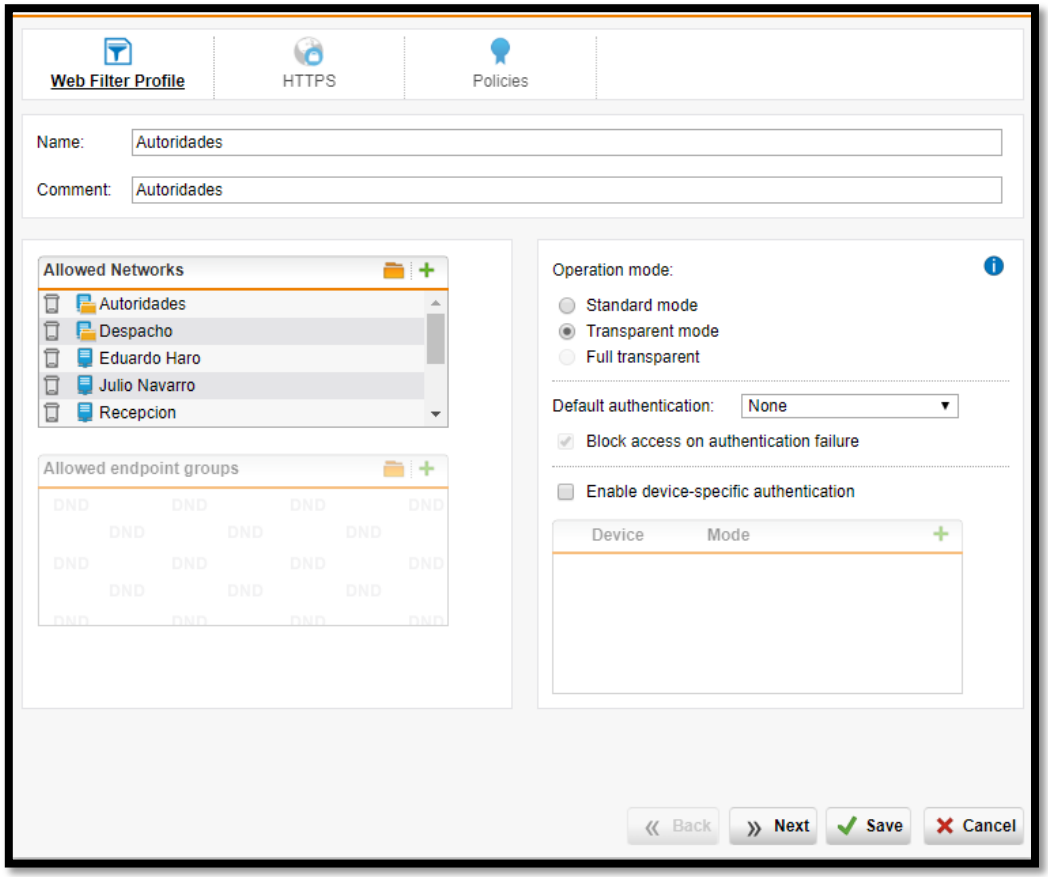


Figura 202. Agregar políticas de filtrado.
Elaborado por: Los autores.

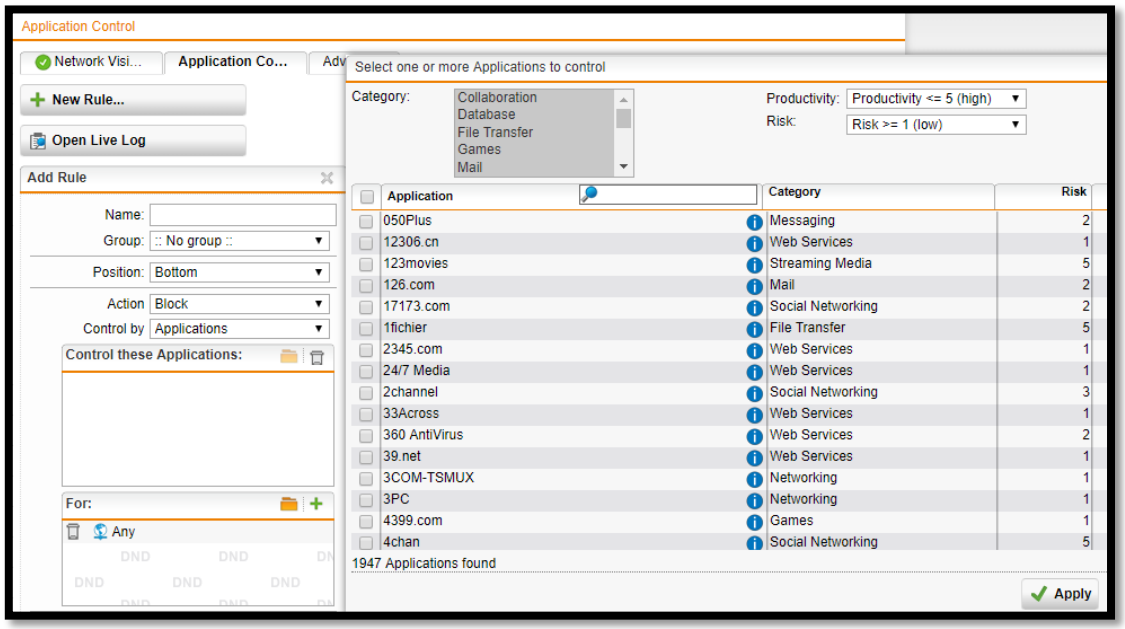


Figura 203. Agregar regla para control de aplicaciones.
Elaborado por: Los autores.

Se configuró también excepciones para la recepción de correos y las direcciones de los servidores de la institución para su respectiva protección.

Email Protection

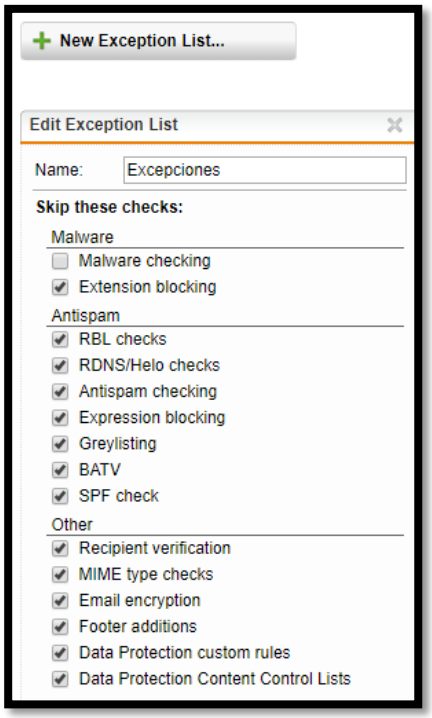


Figura 204. Agregar lista de excepciones para correo.
Elaborado por: Los autores.

Webserver Protection

Figura 205. Agregar servidores para la protección.
Elaborado por: Los autores.

10.6. Anexo F: Planos y detalle de puntos de red por departamentos

- Planta Baja

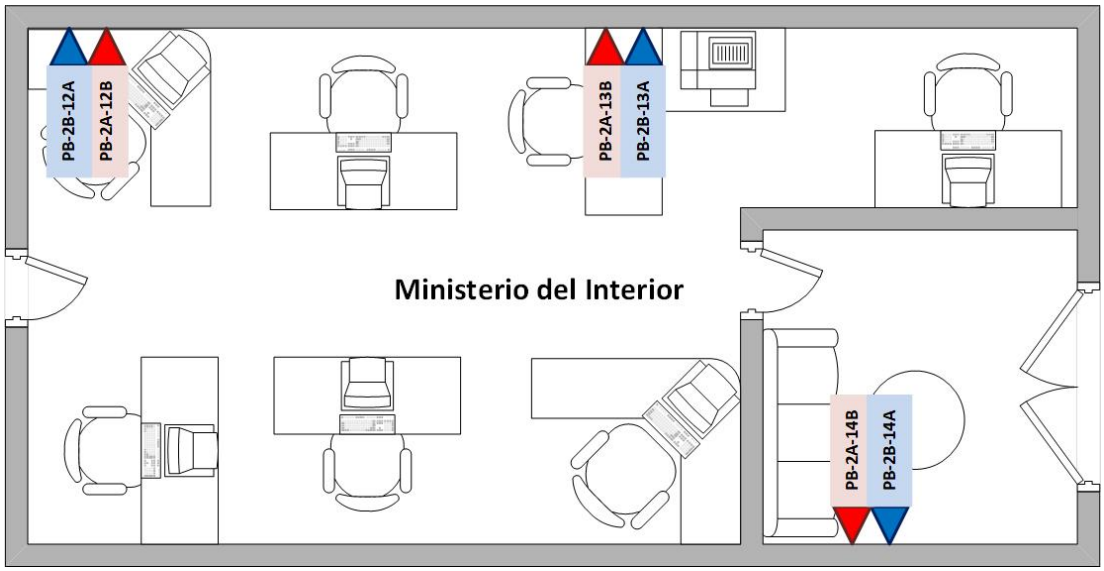


Figura 206. Plano de Ministerio del Interior.
Elaborado por: Los autores.

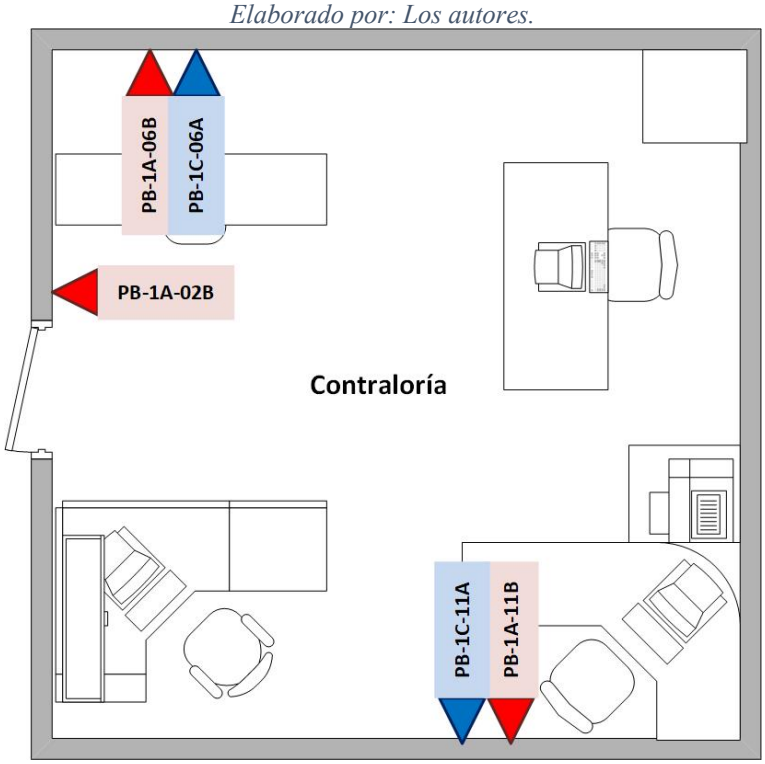


Figura 207. Plano de Contraloría.
Elaborado por: Los autores.

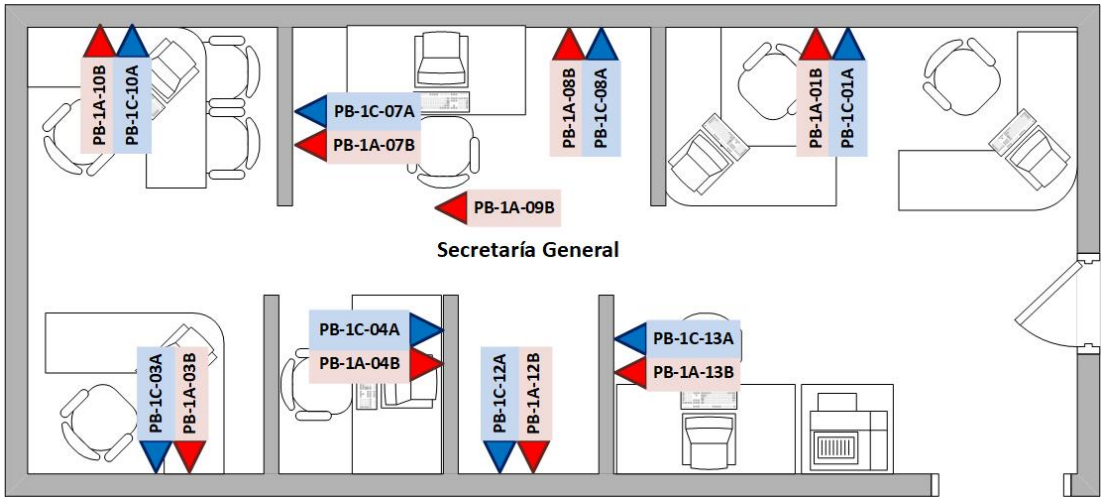


Figura 208. Plano de Secretaría General.
Elaborado por: Los autores.

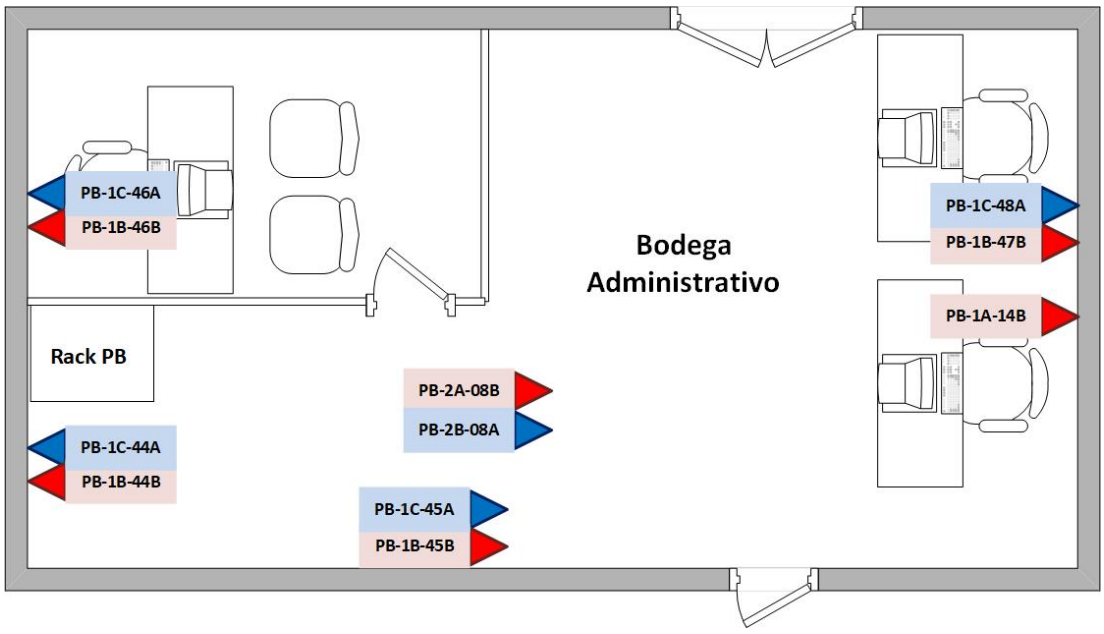


Figura 209. Plano de Bodega administrativa.
Elaborado por: Los autores.

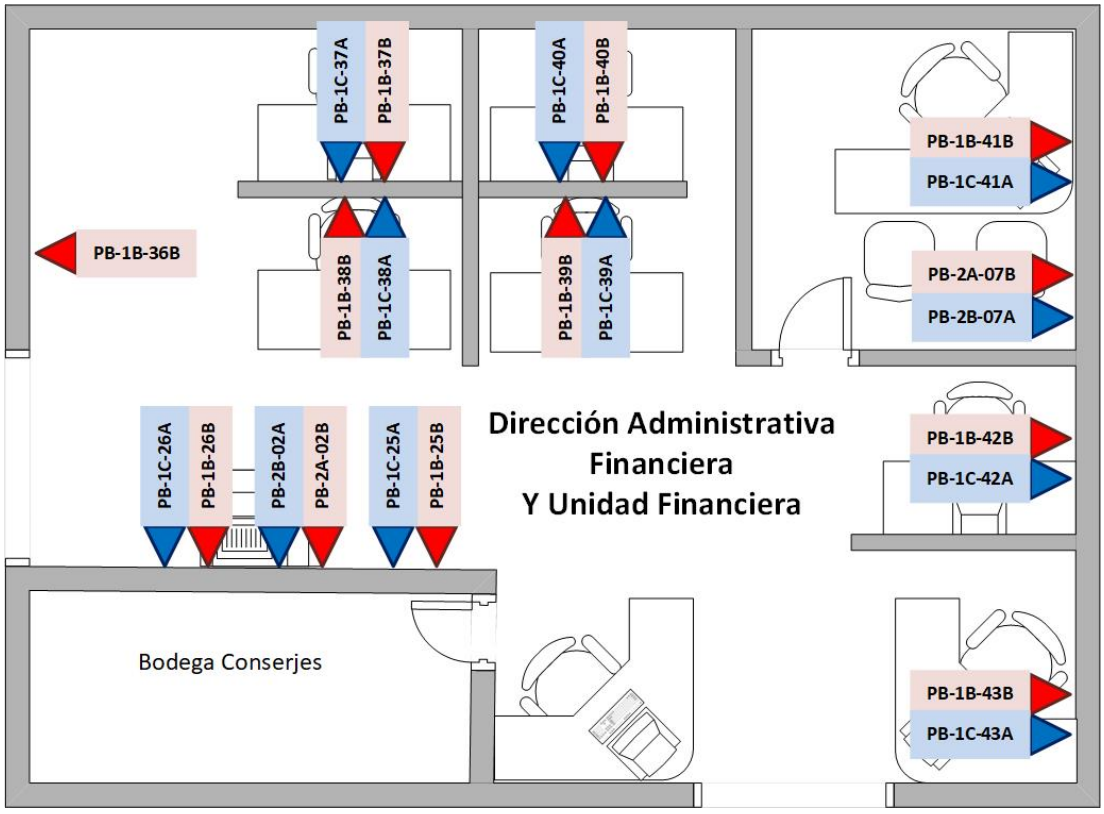


Figura 210. Plano de Dirección Administrativa Financiera y Unidad Financiera.
Elaborado por: Los autores.

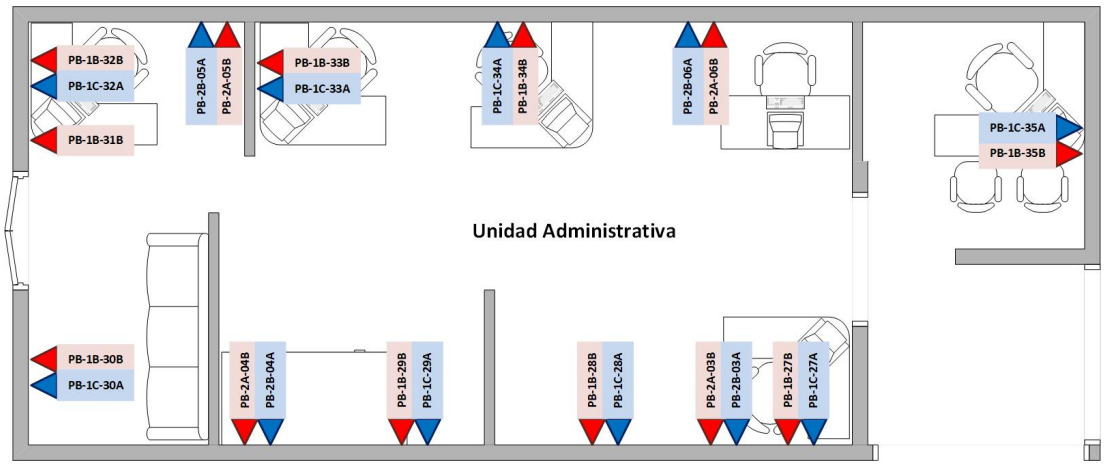


Figura 211. Plano de Unidad Administrativa.
Elaborado por: Los autores.

- Primer Piso

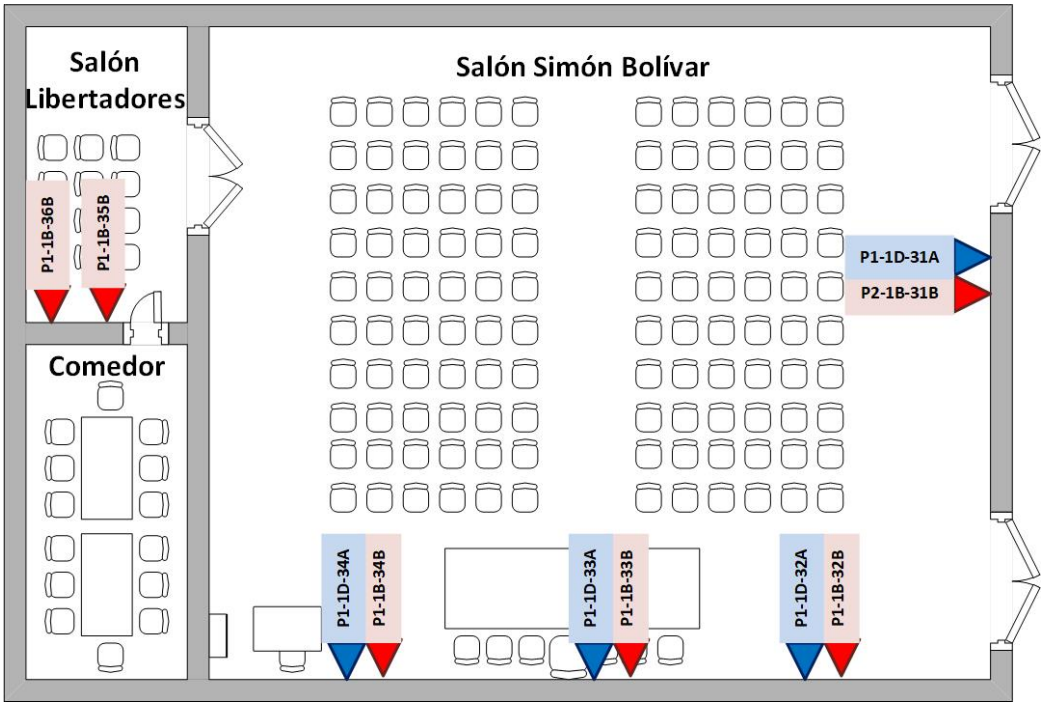


Figura 212. Plano de Salón Simón Bolívar.
Elaborado por: Los autores.

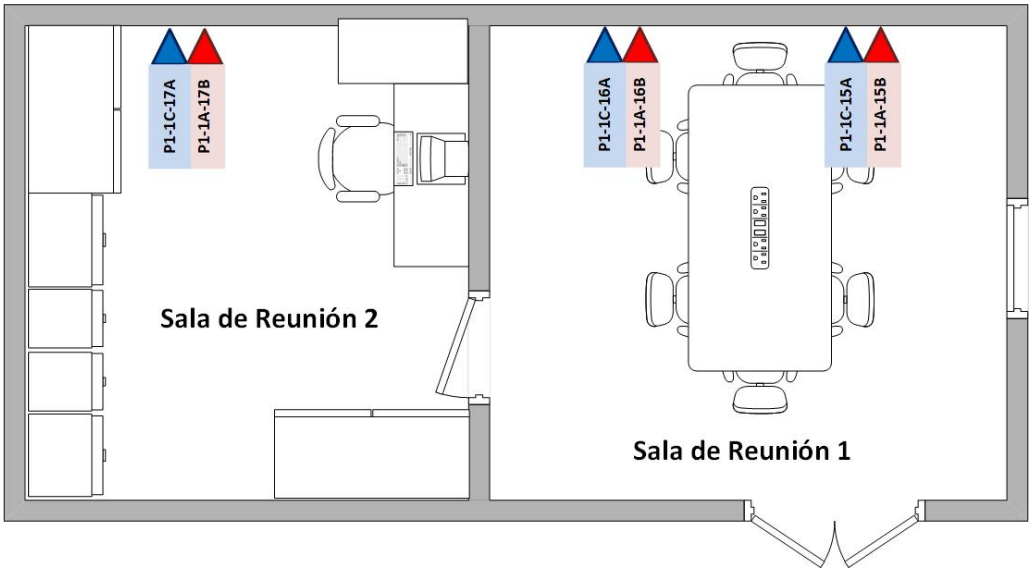


Figura 213. Plano de Sala de Reunión 1 y 2
Elaborado por: Los autores.

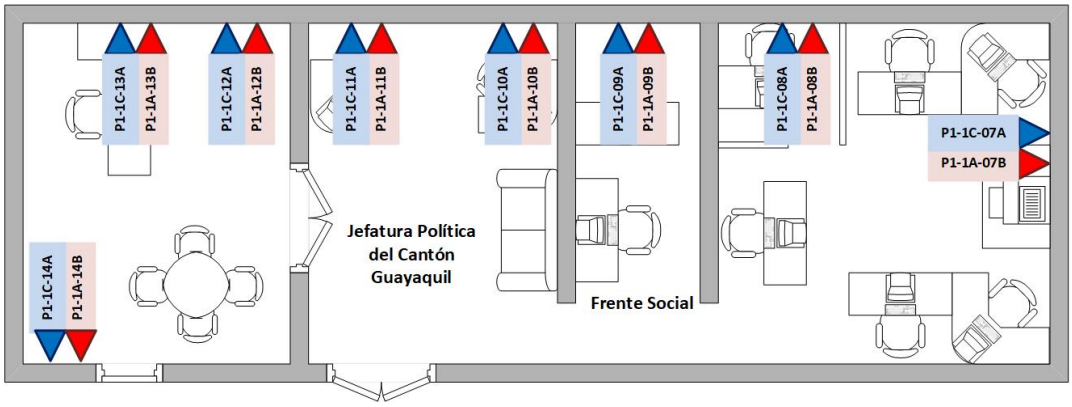


Figura 214. Plano de Jefatura Política y Frente Social.
Elaborado por: Los autores.

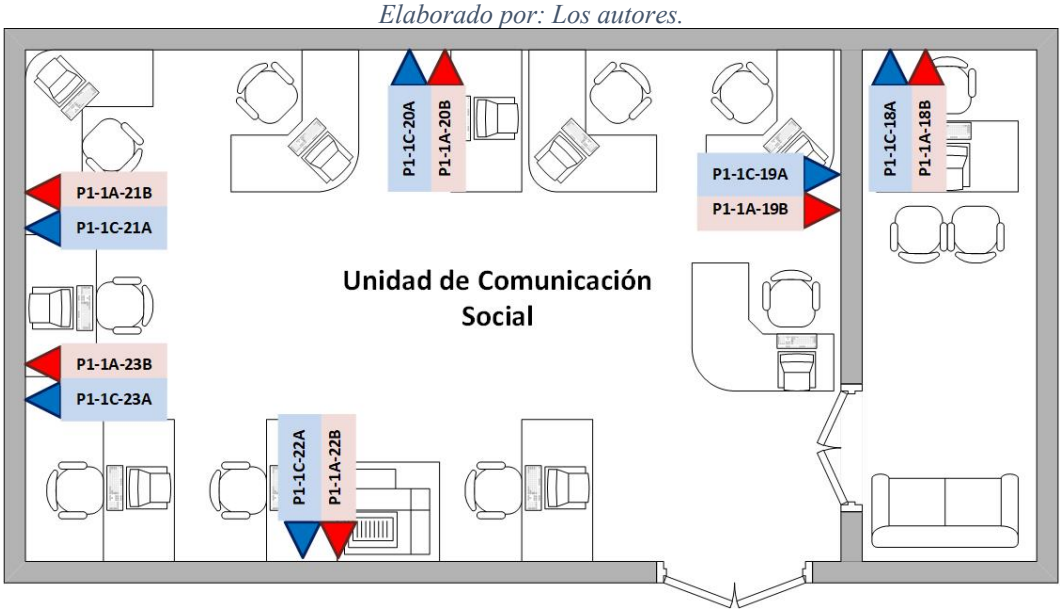


Figura 215. Plano de Unidad de Comunicación.
Elaborado por: Los autores.

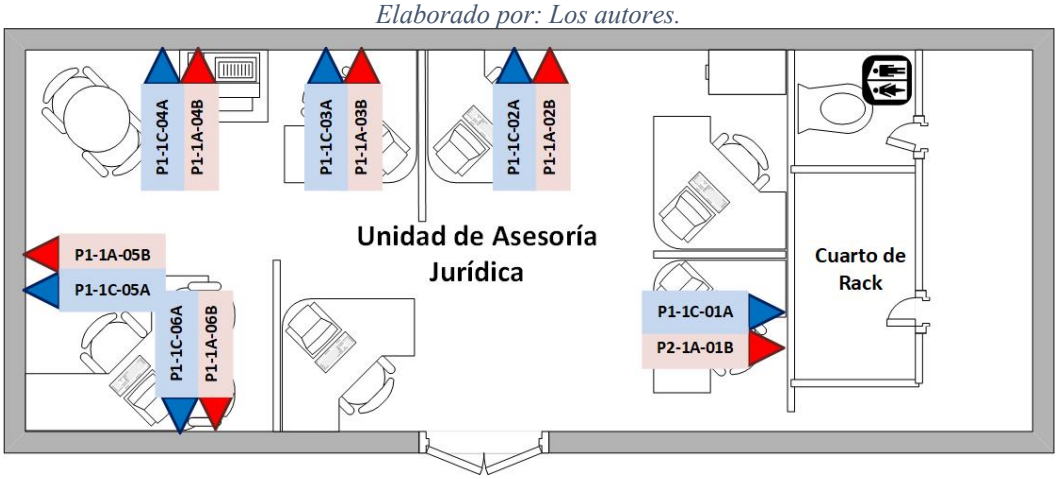


Figura 216. Plano de Unidad de Asesoría Jurídica.
Elaborado por: Los autores.

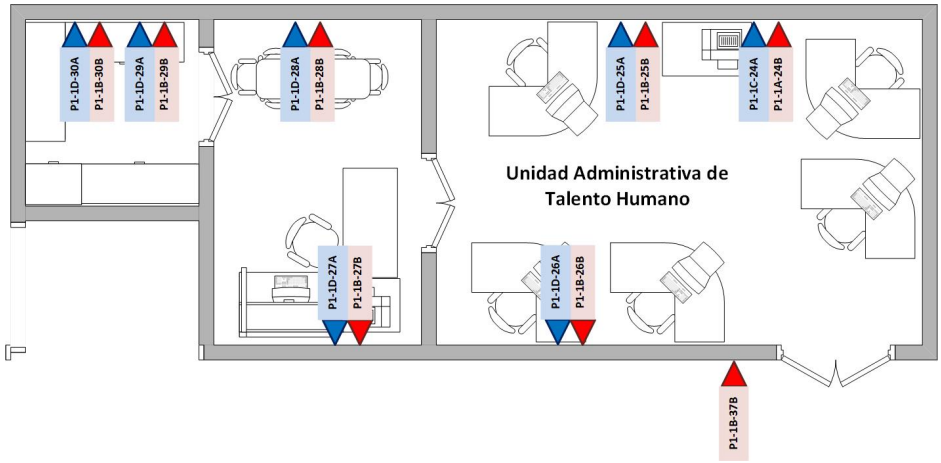


Figura 217. Plano de Unidad de Talento Humano.
Elaborado por: Los autores.

- Segundo Piso

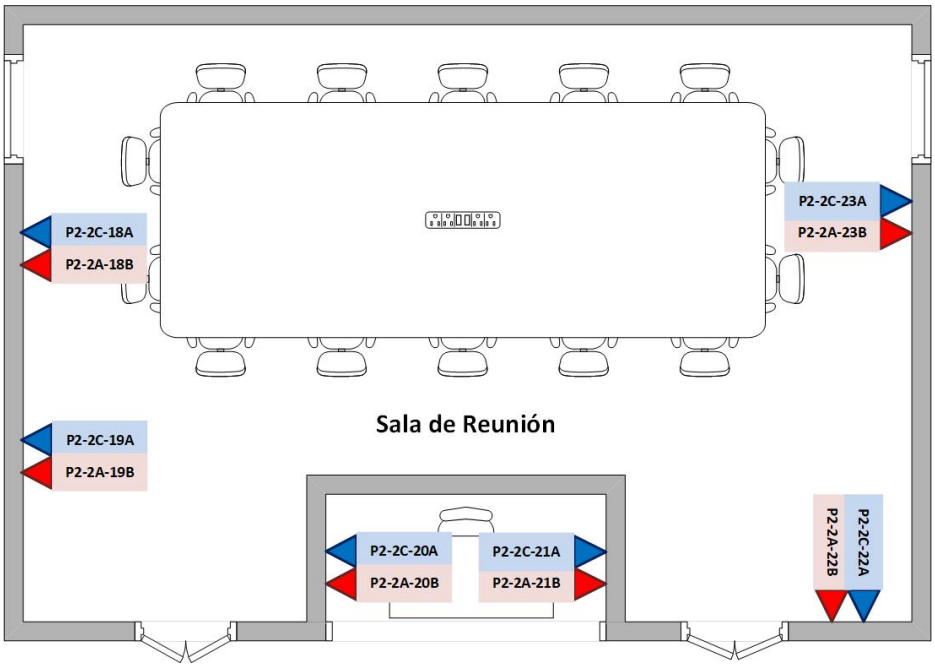


Figura 218. Plano de Sala de Reunión.
Elaborado por: Los autores.

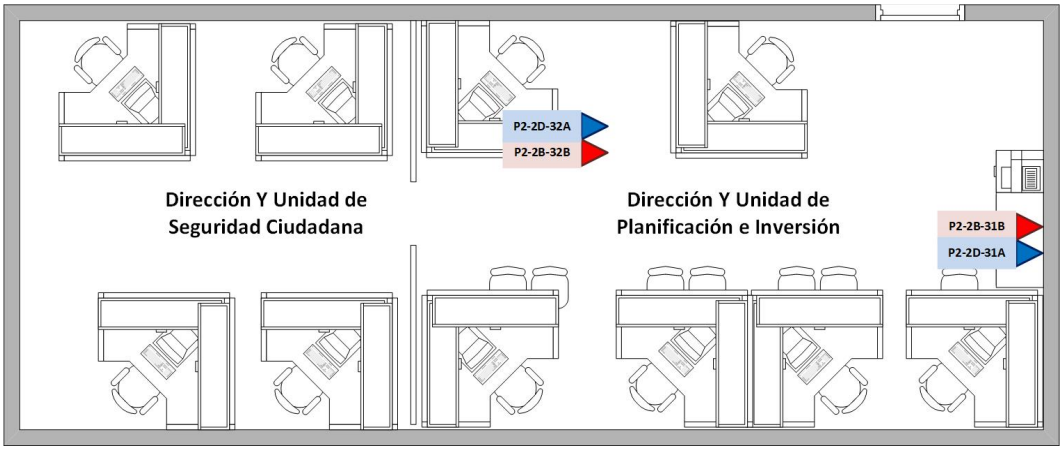


Figura 219. Plano de Dirección y Unidad de: Seguridad Ciudadana y Planificación e Inversión.
Elaborado por: Los autores.

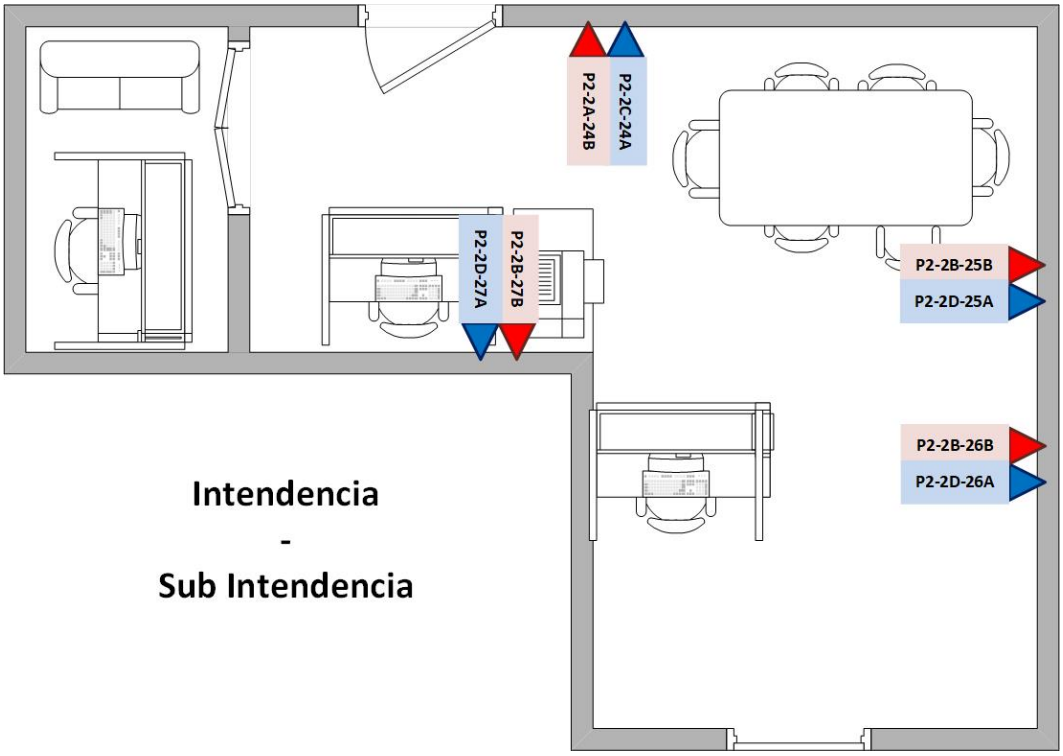


Figura 220. Plano de Intendencia y Subintendencia.
Elaborado por: Los autores.

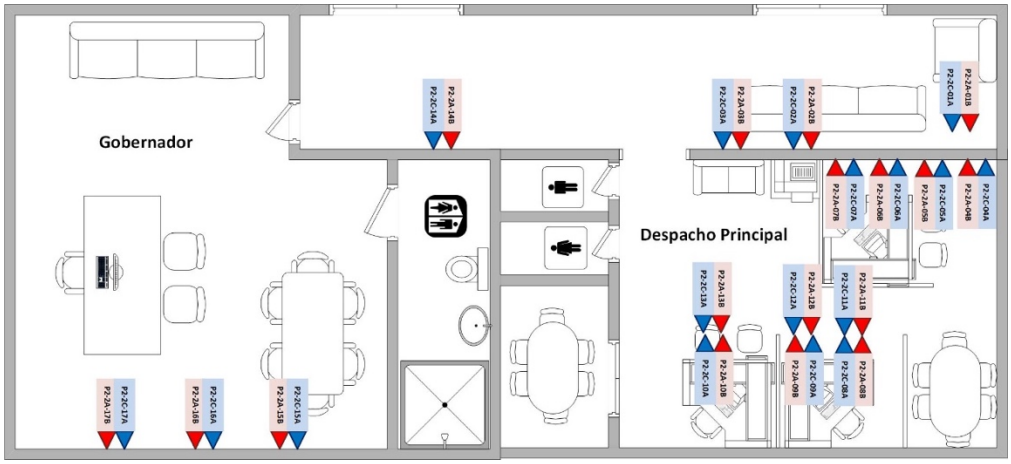


Figura 221. Planos de Despacho del Gobernador.
Elaborado por: Los autores.

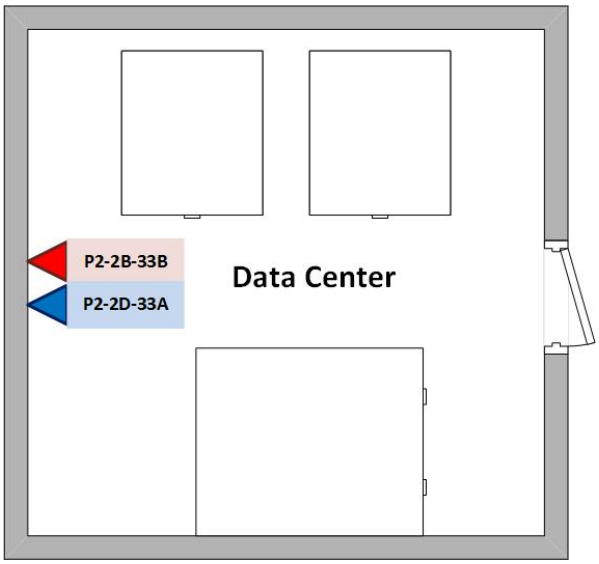


Figura 222. Plano del Data Center.
Elaborado por: Los autores.

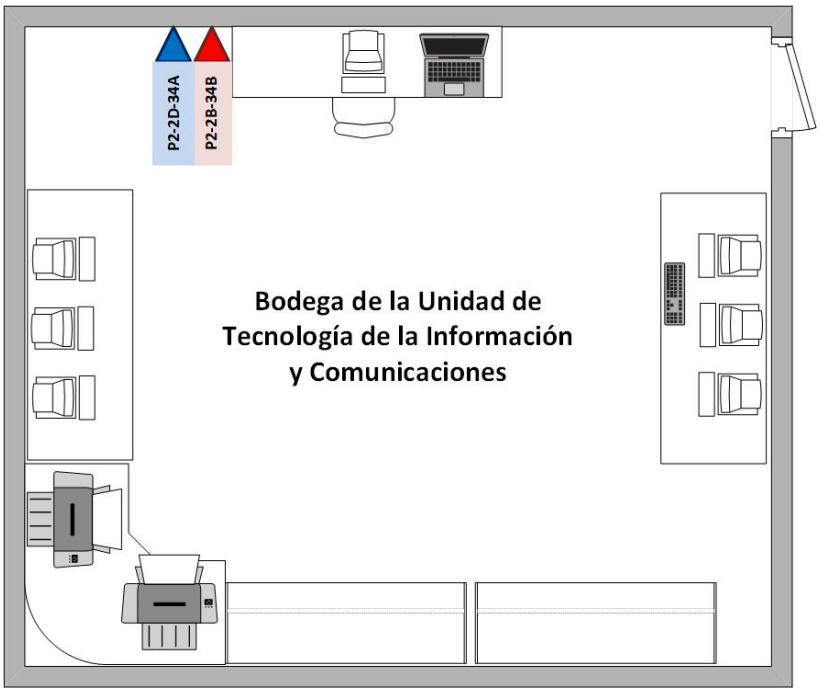


Figura 223. Bodega de la Unidad de Tecnología de la Información y Comunicaciones.
Elaborado por: Los autores.

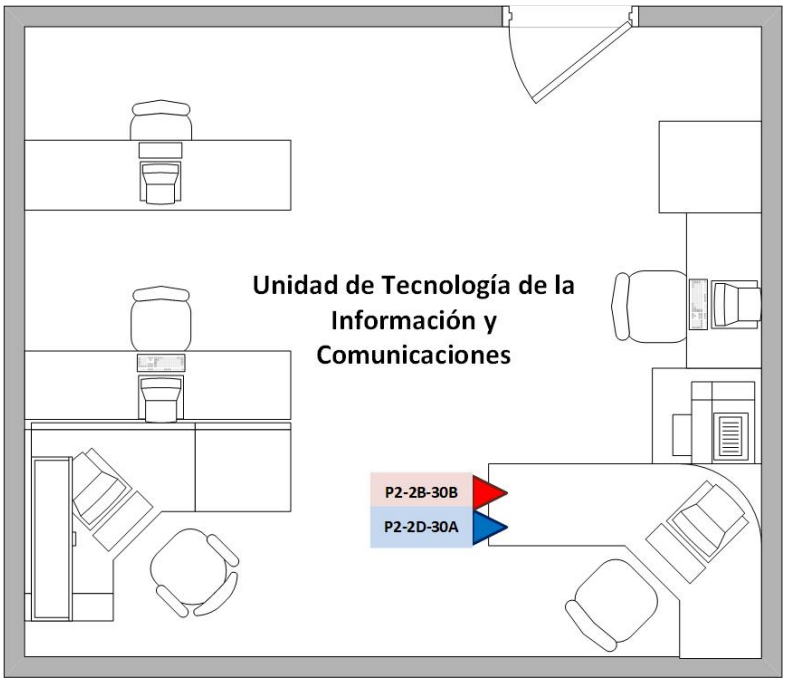


Figura 224. Unidad de Tecnología de la Información y Comunicaciones.
Elaborado por: Los autores.